

Docket No.: 60188-790

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
	:	
Ikuko FUJINAWA, et al.	:	Confirmation Number:
	:	
Serial No.:	:	Group Art Unit:
	:	
Filed: March 3, 2004	:	Examiner:
	:	
For: DATA PROCESSING DEVICE AND DATA PROCESSING METHOD	:	

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

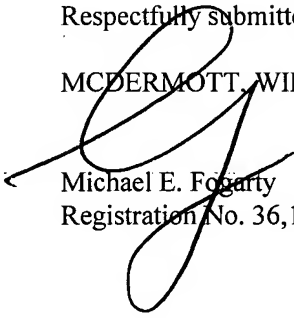
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. JP 2003-055626, filed on March 3, 2003.

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:gav
Facsimile: (202) 756-8087
Date: March 3, 2004

60188-790
IKUKO FUJINAWA et al.
March 3, 2004

McDermott, Will & Emery

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 3 月 3 日

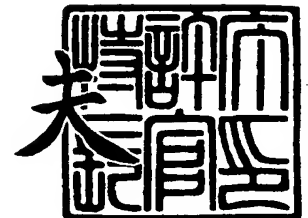
出 願 番 号
Application Number: 特 願 2 0 0 3 - 0 5 5 6 2 6
[ST. 10/C]: [J P 2 0 0 3 - 0 5 5 6 2 6]

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 3 年 9 月 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 3 4 0 8

【書類名】 特許願

【整理番号】 5037720199

【提出日】 平成15年 3月 3日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/14 320
G09C 1/00 310

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 藤縄 幾子

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 樋口 淑夫

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【選任した代理人】

【識別番号】 100117581

【弁理士】

【氏名又は名称】 二宮 克也

【選任した代理人】

【識別番号】 100117710

【弁理士】

【氏名又は名称】 原田 智雄

【選任した代理人】

【識別番号】 100121500

【弁理士】

【氏名又は名称】 後藤 高志

【選任した代理人】

【識別番号】 100121728

【弁理士】

【氏名又は名称】 井関 勝守

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0217869

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置、および情報処理方法

【特許請求の範囲】

【請求項 1】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および
上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記暗号化データおよび暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項 2】

請求項 1 の情報処理装置であって、

上記読み込み制御部は、
全ての上記分割データがそれぞれ暗号化されて上記記憶媒体に記憶された各暗号化データと、上記暗号化データをそれぞれ復号化する鍵データが暗号化されて上記記憶媒体に記憶された各暗号化鍵データとを、所定の一意に定まった順序で順次読み込むように構成され、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記記憶媒体から読み込まれた第 1 の暗号化データおよび第 1 の暗号化鍵データを復

号化して、第1の分割データおよび第1の鍵データを出力するとともに、復号化されて上記鍵データ保持部に保持された上記第1の鍵データに基づいて、上記第1の暗号化データおよび第1の暗号化鍵データに後続して読み込まれた、第2の暗号化データおよび第2の暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項3】

請求項1の情報処理装置であって、
上記読み込み制御部は、
上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、
他の分割データが暗号化されことなく上記記憶媒体に記憶された非暗号化データ、および
上記各暗号化データおよび非暗号化データにそれぞれ対応して上記記憶媒体に記憶された暗号化鍵データを、
所定の一意に定まった順序で順次読み込むように構成されるとともに、
上記復号化部は、
上記記憶媒体から第1の暗号化鍵データと第1の暗号化データとが読み込まれた場合には、
これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第1の分割データおよび第1の鍵データを出力する一方、
上記記憶媒体から第1の暗号化鍵データと第1の非暗号化データとが読み込まれた場合には、
上記第1の暗号化鍵データを上記鍵データ保持部に保持された鍵データに基づき復号化して、第1の鍵データを出力し、
上記第1の暗号化鍵データと第1の暗号化データと、または上記第1の暗号化鍵データと第1の非暗号化データとに後続して読み込まれた、第2の暗号化鍵データ、または第2の暗号化鍵データと第2の暗号化データとを、上記第1の鍵データに基づいて復号化するように構成されていることを特徴とする情報処理装置。

【請求項4】

請求項 1 の情報処理装置であって、

上記読み込み制御部は、

上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、

他の分割データが暗号化されることなく上記記憶媒体に記憶された非暗号化データ、および

上記各暗号化データに対応して上記記憶媒体に記憶された暗号化鍵データを、所定の一意に定まった順序で順次読み込むように構成されるとともに、

上記復号化部は、

上記記憶媒体から第 1 の暗号化鍵データおよび第 1 の暗号化データが読み込まれた場合には、

これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第 1 の分割データおよび第 1 の鍵データを出力するとともに、

上記第 1 の暗号化鍵データおよび第 1 の暗号化データ以降に読み込まれた、第 2 の暗号化鍵データおよび第 2 の暗号化データを、上記第 1 の鍵データに基づいて復号化するように構成されていることを特徴とする情報処理装置。

【請求項 5】

請求項 1 の情報処理装置であって、

上記読み込み制御部は、上記記憶媒体に記憶された第 1 の暗号化データに後続して、上記第 1 の暗号化データに対応してあらかじめ定まった 1 つ以上の第 2 の暗号化データから成る後続候補群のうちの何れかの第 2 の暗号化データを読み込むとともに、

上記第 1 の暗号化データに対応して、それぞれ上記後続候補群の各第 2 の暗号化データを復号化するための鍵データが暗号化された 1 つ以上の暗号化鍵データを含む暗号化鍵データ群を読み込むように構成され、

上記鍵データ保持部は、上記記憶媒体から読み込まれた上記暗号化鍵データ群の各暗号化鍵データから復号化された 1 つ以上の鍵データを保持し、

上記復号化部は、鍵データ保持部に保持された上記 1 つ以上の鍵データのうち、上記第 1 の暗号化データに後続して実際に読み込まれた第 2 の暗号化データに

対応する鍵データに基づいて、上記第2の暗号化データ、およびその第2の暗号化データに対応して読み込まれた暗号化鍵データ群の各暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項6】

請求項2から請求項5のうちの何れか1項の情報処理装置であって、

上記記憶媒体に記憶されるべきデータは、上記情報処理装置に実行させる命令を含み、上記暗号化データおよび非暗号化データの読み込み順序が、上記命令のうちの分岐命令によって決定されることを特徴とする情報処理装置。

【請求項7】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データ、および上記共通鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項8】

請求項7の情報処理装置であって、

上記鍵データ保持部は、上記暗号化鍵データから復号化された鍵データを保持する第1の鍵データ保持部と、上記共通鍵データを保持する第2の鍵データ保持

部とを備え、

上記復号化部は、上記第 1 の鍵データ保持部に保持された鍵データに基づいて上記暗号化データを復号化する第 1 の復号化部と、上記第 2 の鍵データ保持部に保持された共通鍵データに基づいて上記暗号化鍵データを復号化する第 2 の復号化部とを備えたことを特徴とする情報処理装置。

【請求項 9】

請求項 8 の情報処理装置であって、

さらに、上記第 2 の復号化部によって上記暗号化鍵データの復号化が行われる間に、上記記憶媒体に対して、次に読み込むべきデータとは異なる領域に記憶されているデータを読み込むのと同じ信号を出力する擬似読み込み信号出力部を備えたことを特徴とする情報処理装置。

【請求項 1 0】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方法であって、

上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと

上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵データを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持部に保持させる復号化ステップとを有し、

上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化することを特徴とする情報処理方法。

【請求項 1 1】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも

一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方法であって、

上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと

上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵データを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持部に保持させる復号化ステップとを有し、

上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化することを特徴とする情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、メモリや、ＩＣカード、ハードディスクなどの記憶媒体に記憶されたデータが容易に第三者に漏洩することの防止に関する技術に属する。

【0002】

【従来の技術】

従来より、メモリなどの記憶媒体に記憶されたデータ、特にＣＰＵに実行させる一連の命令コードから成るプログラムとしてのデータが第三者に漏洩するのを防ぐために、データの暗号化を用いる技術が知られている。具体的には、例えば特許文献１に記載されているように、あらかじめ、記憶媒体に記憶されたデータを読み出す装置に固定的に設定され、または記憶データごとに任意に設定された暗号鍵（復号鍵）を用い、記憶媒体から読み出された暗号化されたデータを順次復号化して、装置内のＣＰＵに入力するように構成したデータ保護装置が知られている。

【0003】

【特許文献1】

特開平7-129473号公報

【0004】

【発明が解決しようとする課題】

しかしながら、上記のような従来の装置では、暗号化されたデータを復号化する暗号鍵として単一の暗号鍵が用いられているために、復号化方法（アルゴリズム）とともに、1つの暗号鍵が漏洩してしまうと、記憶媒体に記憶されている全てのデータが漏洩してしまうという問題が生じる。

【0005】

なお、上記のような全てのデータの漏洩を防止するためには、記憶媒体に記憶させるデータを複数のブロックに分割し、各ブロックごとに別個の暗号鍵を用いて暗号化、復号化を行うようにすることも考えられるが、そのためには、複数の暗号鍵を各ブロックと対応づけて扱う必要があり、暗号化、復号化処理や暗号鍵の管理の複雑化を招くことになる。

【0006】

上記の問題に鑑み、本発明は、暗号鍵の管理の複雑化などを招くことなく、記憶媒体に記憶されたデータが容易に第三者に漏洩するのを防止可能にすることを課題とする。

【0007】

【課題を解決するための手段】

前記の課題を解決するために、請求項1の発明が講じた解決手段は、
記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および
上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記暗号化データおよび暗号化鍵データを復号化するように構成されていることを特徴とする。

【0 0 0 8】

これによると、各分割データが、それぞれ異なる鍵データによって復号化されるように暗号化されているので、万一、一部の鍵データが漏洩したとしても、記憶媒体の記憶内容全体を容易に知られてしまうことがない。しかも、各鍵データは、それぞれ他の鍵データによって復号化されるように暗号化されて記憶媒体に記憶されているので、複数の鍵データを管理する必要がなく、管理の複雑化を招くことがない。

【0 0 0 9】

また、請求項 2 の発明は、

請求項 1 の情報処理装置であって、

上記読み込み制御部は、

全ての上記分割データがそれぞれ暗号化されて上記記憶媒体に記憶された各暗号化データと、上記暗号化データをそれぞれ復号化する鍵データが暗号化されて上記記憶媒体に記憶された各暗号化鍵データとを、所定の一意に定まった順序で順次読み込むように構成され、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記記憶媒体から読み込まれた第 1 の暗号化データおよび第 1 の暗号化鍵データを復号化して、第 1 の分割データおよび第 1 の鍵データを出力するとともに、復号化されて上記鍵データ保持部に保持された上記第 1 の鍵データに基づいて、上記第 1 の暗号化データおよび第 1 の暗号化鍵データに後続して読み込まれた、

第2の暗号化データおよび第2の暗号化鍵データを復号化するように構成されていることを特徴とする。

【0010】

これによると、記憶媒体に記憶された各暗号化データと各暗号化鍵データとが所定の順序で読み込まれることにより、各暗号化データ、および次の暗号化データを復号化するための暗号化鍵データが順次読み込まれて復号化されるので、暗号化前の元のデータを容易に得ることができる。

【0011】

また、請求項3の発明は、
請求項1の情報処理装置であって、
上記読み込み制御部は、
上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、
他の分割データが暗号化されことなく上記記憶媒体に記憶された非暗号化データ、および
上記各暗号化データおよび非暗号化データにそれぞれ対応して上記記憶媒体に記憶された暗号化鍵データを、
所定の一意に定まった順序で順次読み込むように構成されるとともに、
上記復号化部は、
上記記憶媒体から第1の暗号化鍵データと第1の暗号化データとが読み込まれた場合には、
これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第1の分割データおよび第1の鍵データを出力する一方、
上記記憶媒体から第1の暗号化鍵データと第1の非暗号化データとが読み込まれた場合には、
上記第1の暗号化鍵データを上記鍵データ保持部に保持された鍵データに基づき復号化して、第1の鍵データを出力し、
上記第1の暗号化鍵データと第1の暗号化データと、または上記第1の暗号化鍵データと第1の非暗号化データとに後続して読み込まれた、第2の暗号化鍵デー

タ、または第2の暗号化鍵データと第2の暗号化データとを、上記第1の鍵データに基づいて復号化するように構成されていることを特徴とする。

【0012】

これによると、混在して記憶された暗号化データと非暗号化データとが読み込まれるようにすることにより、復号化動作を最小限に抑えて、読み込み速度の低下を防止することが容易にできる。

【0013】

また、請求項4の発明は、
請求項1の情報処理装置であって、
上記読み込み制御部は、
上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、
他の分割データが暗号化されことなく上記記憶媒体に記憶された非暗号化データ、および
上記各暗号化データに対応して上記記憶媒体に記憶された暗号化鍵データを、
所定の一意に定まった順序で順次読み込むように構成されるとともに、
上記復号化部は、
上記記憶媒体から第1の暗号化鍵データおよび第1の暗号化データが読み込まれた場合には、
これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第1の分割データおよび第1の鍵データを出力するとともに、
上記第1の暗号化鍵データおよび第1の暗号化データ以降に読み込まれた、第2の暗号化鍵データおよび第2の暗号化データを、上記第1の鍵データに基づいて復号化するように構成されていることを特徴とする。

【0014】

これによると、各鍵データは、次に読み込まれる暗号化データおよびこれに対応する暗号化鍵データの復号化に用いられ、非暗号化データに対応する暗号化鍵データを復号化することなどが必要ないので、より、読み込み速度の低下を防止したり、記憶データ量の増加を小さく抑えたりすることができる。

【0015】

また、請求項5の発明は、

請求項1の情報処理装置であって、

上記読み込み制御部は、上記記憶媒体に記憶された第1の暗号化データに後続して、上記第1の暗号化データに対応してあらかじめ定まった1つ以上の第2の暗号化データから成る後続候補群のうちの何れかの第2の暗号化データを読み込むとともに、

上記第1の暗号化データに対応して、それぞれ上記後続候補群の各第2の暗号化データを復号化するための鍵データが暗号化された1つ以上の暗号化鍵データを含む暗号化鍵データ群を読み込むように構成され、

上記鍵データ保持部は、上記記憶媒体から読み込まれた上記暗号化鍵データ群の各暗号化鍵データから復号化された1つ以上の鍵データを保持し、

上記復号化部は、鍵データ保持部に保持された上記1つ以上の鍵データのうち、上記第1の暗号化データに後続して実際に読み込まれた第2の暗号化データに対応する鍵データに基づいて、上記第2の暗号化データ、およびその第2の暗号化データに対応して読み込まれた暗号化鍵データ群の各暗号化鍵データを復号化するように構成されていることを特徴とする。

【0016】

また、請求項6の発明は、

請求項2から請求項5のうちの何れか1項の情報処理装置であって、

上記記憶媒体に記憶されるべきデータは、上記情報処理装置に実行させる命令を含み、上記暗号化データおよび非暗号化データの読み込み順序が、上記命令のうちの分岐命令によって決定されることを特徴とする。

【0017】

これらによると、分岐命令の実行などによって、各暗号化データの読み込み順序が一意に定まらないような場合でも、各暗号化データの次に読み込まれる可能性のある各暗号化データを復号化するための鍵データが復号化されて保持されるので、何れの暗号化データが読み込まれる場合でも適切に復号化されるようにすることができる。それゆえ、柔軟な順序で暗号化データを読み込ませることがで

き、したがって、記憶媒体に記憶させるデータの作成や分割を柔軟に行うことなどができる。

【0018】

また、請求項7の発明は、

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データ、および上記共通鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化するように構成されていることを特徴とする。

【0019】

これによると、各暗号化鍵データは、共通鍵データによって復号化されるので、暗号化データや暗号化鍵データの読み込み順序には依存せずに復号化することができる。それゆえ、やはり、柔軟な順序で暗号化データを読み込ませることなどができる。

【0020】

また、請求項8の発明は、

請求項7の情報処理装置であって、

上記鍵データ保持部は、上記暗号化鍵データから復号化された鍵データを保持

する第1の鍵データ保持部と、上記共通鍵データを保持する第2の鍵データ保持部とを備え、

上記復号化部は、上記第1の鍵データ保持部に保持された鍵データに基づいて上記暗号化データを復号化する第1の復号化部と、上記第2の鍵データ保持部に保持された共通鍵データに基づいて上記暗号化鍵データを復号化する第2の復号化部とを備えたことを特徴とする。

【0021】

これによると、暗号化データまたは暗号化鍵データを復号化するための復号化部や鍵データ保持部が別個に設けられることによって、暗号化データと暗号化鍵データとを互いに異なるアルゴリズムによって復号化することなどができるので、暗号化強度と読み込み速度とのバランスをとることなどが容易にできる。

【0022】

また、請求項9の発明は、

請求項8の情報処理装置であって、

さらに、上記第2の復号化部によって上記暗号化鍵データの復号化が行われる間に、上記記憶媒体に対して、次に読み込むべきデータとは異なる領域に記憶されているデータを読み込むのと同じ信号を出力する擬似読み込み信号出力部を備えたことを特徴とする。

【0023】

これによると、暗号化鍵データの復号化が行われる際に、その復号化によって得られた鍵データにより復号化される次のデータが読み出されるまでにタイムラグがある場合などでも、例えば乱数に基づく疑似的なアドレス信号などが出力されることによって、情報処理装置の外部からは暗号化鍵データの復号化が行われていることを察知することなどが困難になる。それゆえ、悪意の者が解析によって記憶内容を取得することなどを一層困難にすることができる。

【0024】

また、請求項10の発明は、

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号

化された暗号化データ、および
上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化され
た暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方
法であって、

上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと

、
上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵デ
ータを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持
部に保持させる復号化ステップとを有し、

上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データに基づ
いて、上記暗号化データおよび上記暗号化鍵データを復号化することを特徴とす
る。

【0025】

また、請求項11の発明は、

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも
一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号
化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号
化された暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方
法であって、

上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと

、
上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵デ
ータを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持
部に保持させる復号化ステップとを有し、

上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データまたは
上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復

号化することを特徴とする。

【0026】

これらによっても、前記請求項1や請求項7について説明したように、やはり、鍵データの管理の複雑化を招いたりすることなく、記憶内容の秘匿性を高めることが容易にできる。

【0027】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して説明する。

【0028】

(実施の形態1)

(装置の構成)

図1は本発明の実施の形態1に係る情報処理装置の例としてのマイクロコンピュータ100の要部の構成、および上記マイクロコンピュータ100に接続された記憶媒体としてのメモリ120を示すブロック図である。

【0029】

上記メモリ120は、例えばROMやRAMによって構成され、マイクロコンピュータ100に実行させる命令の命令コードから成るプログラムが暗号化されたデータを記憶し、アドレスバスによって示されるアドレスに応じたデータをデータバスに出力するようになっている。このメモリ120には、例えば図2に示すように、一連の命令コードから成るプログラム（データ）が5つのデータブロック201～205として記憶されているが、その記憶形式については、後に詳述する。

【0030】

マイクロコンピュータ100には、CPU101（読み込み制御部）と、復号化部102と、鍵データ保持部103と、選択部104と、選択指示保持部105と、復号化情報管理部106とが設けられている。

【0031】

上記CPU101は、命令コードの実行処理を行うものである。このCPU101には、復号化制御部101aが設けられている。上記復号化制御部101a

は、メモリ 120 に記憶された各データブロック 201～205 が読み込まれる際に、各データブロック 201～205 に含まれる復号化情報 211～215 を読み込んで、鍵データ（復号鍵）等を復号化情報管理部 106 に出力するなどの制御を行うようになっている。

【0032】

復号化部 102 は、鍵データ保持部 103 に設定された鍵データを用いて、メモリ 120 から出力された暗号化データを復号化するものである。

【0033】

選択部 104 は、選択指示保持部 105 に設定された選択指示に基づいて、上記復号化部 102 から復号化されて出力されるデータ、またはメモリ 120 から直接出力された（平文の）データの何れか一方を選択し、内部バスを介して CPU 101 に入力するようになっている。ただし、CPU 101 から例えば H（High）レベルの復号化情報読み込み信号が入力される場合には、上記選択指示保持部 105 に設定された選択指示に係らず、復号化部 102 の出力を選択するようになっている。

【0034】

復号化情報管理部 106 は、上記鍵データ保持部 103 に設定される鍵データ、および選択指示保持部 105 に設定される選択指示を管理するようになっている。より詳しくは、CPU 101 から（図示しない出力タイミング信号と共に）出力される鍵データを鍵データ一時保持部 106a に一旦保持するとともに、この保持された鍵データを、メモリ 120 から各データブロック 201～205 の復号化情報 211～215 が読み込まれる前に、鍵データ保持部 103 に設定するようになっている。また、CPU 101 から（図示しない出力タイミング信号と共に）出力される選択部 104 への選択指示を選択指示一時保持部 106b に一旦保持するとともに、この保持された選択指示を、各データブロック 201～205 に含まれる実行ブロック 221～225 が読み込まれる前に、選択部 104 に設定するようになっている。（また、上記設定が完了すると、CPU 101 に設定終了信号を出力して、次のアドレスの出力などの動作をさせ得るようになっている。なお、上記設定が例えば 1 クロックサイクル内に行われる場合などに

は、CPU101に次の動作を適切なタイミングで行わせることが容易にできるので、必ずしも上記のような設定終了信号を出力するようにしなくてもよい。) 上記鍵データ一時保持部106a、および選択指示一時保持部106bには、上記のようにCPU101から出力された鍵データ等が一旦保持される他、さらに、最初のデータブロックが読み込まれる際にマイクロコンピュータ100の外部から入力された鍵データ等が保持されるようになっている。

【0035】

ここで、メモリ120に記憶されるデータの暗号化方式としては種々のものを適用することができ、特に限定されないが、例えば、DES暗号方式のように1つの暗号鍵によって暗号化および復号化が行われる、可逆変換が可能な共通鍵暗号方式や、暗号鍵を初期値として、順次入力されるデータの排他的論理和演算を行う方式などを用いることができる。

【0036】

なお、マイクロコンピュータ100には、通常、上記の他にも、一時的なデータ等を保持するRAMや、外部の装置との間で入出力を行うインタフェース、また、メモリ120がデータの書き込みも可能な記憶媒体である場合には書き込み制御部などを備えているが、本発明の主眼ではないのでここでは省略する。

【0037】

また、マイクロコンピュータ100は、例えば1チップのLSIで構成される場合には、上記各部間の信号を解析することなどが一層困難になるので、より秘匿性を高めることができるが、これに限るものではない。

【0038】

(メモリ120に記憶されるデータの形式)

メモリ120には、図2に示すように、それぞれ復号化情報211～215と実行ブロック221～225とを含む複数(同図の例では5つ)のデータブロック201～205が記憶されている。これらのデータブロック201～205のCPU101への読み込みは、データブロック201～205に含まれるポイント等に基づいて、あらかじめ定められた一定の順序で行われるようになっている。(ここでは説明の簡単化のために、データブロック201～205の順で読み

込まれるとして説明する。)

上記実行ブロック 2 2 1 ~ 2 2 5 は、例えば図 3 に示すように、一連の命令コードから成るプログラム（データ）が 5 つの実行単位に分割された命令コード列 2 2 1 a ~ 2 2 5 a に実行終了コード 2 3 0 が付加されて構成されている。上記実行終了コード 2 3 0 としては、具体的には、例えば分岐先のデータブロックを特定して分岐する専用の命令を用いたり、通常に分岐命令と、分岐先が他のデータブロックであることを示すフラグをセットする命令とを組み合わせ用いたり、通常に分岐命令を用いて、分岐先のアドレスなどによって CPU 1 0 1 が他のデータブロックへの分岐であることを検出し得るようにしたりしてもよい。さらに、通常に分岐命令で他のデータブロックのアドレスに分岐した後に、分岐先のデータブロックまたは実行ブロックの先頭に、データブロックが変わったことを示す（復号化情報の読み込みなどの処理をさせる）命令を設けるなどしてもよい。なお、分岐先のデータブロックをアドレスによって特定する場合、そのアドレスとしては、復号化情報の先頭のアドレスを指定するようにしてもよいし、実行ブロックの先頭のアドレス等を指定して、復号化情報のデータ長などから復号化情報の先頭のアドレスを求め得るようにしてもよい。

【 0 0 3 9 】

また、復号化情報 2 1 1 ~ 2 1 5 には、それぞれ、鍵データ 2 1 1 a ~ 2 1 5 a と暗号化有無情報 2 1 1 b ~ 2 1 5 b とが含まれている。（なお、復号化情報 2 1 1 ~ 2 1 5 は、データブロック 2 0 1 ~ 2 0 5 の先頭に限らず、実行ブロック 2 2 1 ~ 2 2 5 の内部や末尾などに配置されるようにしてもよい。また、データブロック 2 0 5 の次に読み込まれるデータブロックがない場合、すなわち、データブロック 2 0 5 内の命令が繰り返し実行されて、他のデータブロックに移行しない場合には、鍵データ 2 1 5 a および暗号化有無情報 2 1 5 b の内容は不定でよく、さらに、これらの情報を省略することもできる。）

上記復号化情報 2 1 1 ~ 2 1 5 は全て暗号化されている一方、実行ブロック 2 2 1 ~ 2 2 5 は必要に応じて（例えば実行ブロック 2 2 2 ・ 2 2 4 が）暗号化されている。上記暗号化されたデータを復号化するための鍵データは、それぞれのデータブロック 2 0 1 ~ 2 0 5 ごとに異なり、各データブロック 2 0 2 ~ 2 0 5

を復号化する鍵データは、それぞれのデータブロック 202～205 の直前に読み込まれるデータブロック 201～204 の復号化情報 211～214 に含まれている。すなわち、例えばデータブロック 201 の復号化情報 211 に含まれる鍵データ 211 a によって、次に読み込まれるデータブロック 202 の復号化情報 212 および実行ブロック 222 を復号化することができるようになっている。なお、最初に実行されるデータブロック 201（の少なくとも復号化情報 211）を復号化するための鍵データ 210 a は、メモリ 120 中には記憶されておらず、実行時にマイクロコンピュータ 100 の外部から与えられるようになっている。（ここで、上記鍵データは、必ずしも全てが互いに異ならなくてもよい。すなわち、例えば有限個の鍵データから選択された鍵データが用いられるなどして、一部のデータブロックに同じ鍵データが用いられることがあってもよい。）

また、復号化情報 211～214 に含まれる暗号化有無情報 211 b～214 b は、次のデータブロック 202～205 の実行ブロック 222～225 が暗号化されているかどうかを示し、例えば、各データブロックの次に実行されるデータブロックの実行ブロックが暗号化されている場合には、値 0x0010（「0x」は続く数値が 16 進数表記であることを示す。）が設定される一方、暗号化されていない場合には、値 0x0001 が設定されている。より具体的には、前記のようにデータブロック 202・204 の実行ブロック 222・224 が暗号化されている場合には、これらの直前に読み込まれるデータブロック 201・203 の暗号化有無情報 211 b・213 b には 0x0010 が設定され、その他のデータブロック 202・204 の暗号化有無情報 212 b・214 b には 0x0001 が設定されている。

【0040】

上記のようなデータを生成してメモリ 120 に保存する手順は特に限定されないが、例えば図 4 に示すようにして行うことができる。まず、一連の命令コードから成るプログラムを（例えば所定のデータ長ごと、またはその前後の分岐命令を区切りとして）5 つの命令コード列 221 a～225 a に分割し（S101）、各データブロック 201～205 の復号化情報 211～215 等および実行ブロック 222・224 をそれぞれ暗号化するための鍵データ 210 a～215 a

を乱数を用いるなどして自動的に、または人為的に定め（S102）、上記鍵データ211a～215aと暗号化有無情報211b～215bとを連結して復号化情報211～215を生成し（S103）、上記分割された命令コード列221a～225aに実行終了コード230を付加して実行ブロック221～225を生成するとともに、これらの実行ブロック221～225と復号化情報211～215とをそれぞれ連結してデータブロック201～205を構成し（S104）、全ての復号化情報211～215を鍵データ210a～214aで暗号化し、実行ブロック222・224を鍵データ211a・213aで暗号化して（S105）、メモリ120に格納する（S106）。

【0041】

（メモリ120に記憶されたデータの読み込みと実行動作）

上記のようにメモリ120に記憶されたプログラムがマイクロコンピュータ100に読み込まれて実行される場合の動作について、図5に基づいて説明する。

【0042】

（S201） マイクロコンピュータ100の外部から、最初に読み込まれるデータブロック201についての鍵データ210a、および選択指示が入力されると、これらを復号化情報管理部106の鍵データ一時保持部106a、および選択指示一時保持部106bが保持する。

【0043】

（S202） 復号化制御部101aの制御によって、CPU101が復号化情報管理部106および選択部104にHレベルの復号化情報読み込み信号を出力する。これに応じて、復号化情報管理部106の鍵データ一時保持部106a、および選択指示一時保持部106bに保持されている、鍵データおよび選択指示が、それぞれ鍵データ保持部103または選択指示保持部105に設定される。また、選択部104は、上記選択指示保持部105に設定された選択指示に係らず、復号化部102からの出力を選択して101に出力するように切り替わる。

【0044】

（S203） 復号化制御部101aの制御によって、CPU101がメモリ

120に復号化情報を読み込むためのアドレス（および図示しない読み出し制御信号）を出力する。これに応じて、メモリ120は復号化情報を出力する。

【0045】

(S204) 復号化部102は、メモリ120から出力された復号化情報を鍵データ保持部103に設定された鍵データに基づいて復号化し、選択部104は上記復号化部102の出力を選択してCPU101に入力する。

【0046】

(S205) 復号化制御部101aは、上記復号化情報に含まれる鍵データを抽出して復号化情報管理部106に出力し、鍵データ一時保持部106aに一旦保持させる。また、復号化情報に含まれる暗号化有無情報に基づいて、すなわち、次のデータブロックの実行ブロックが暗号化されているかどうかに応じて、復号化情報管理部106の選択指示一時保持部106bに、復号化部102またはメモリ120の何れからの出力を選択部104に選択させるかを示す選択指示を一旦保持させる。（これらの鍵データおよび選択指示は、次のデータブロックを読み込むために再度（S202）が実行される際に鍵データ保持部103および選択指示保持部105に設定される。）

(S206) マイクロコンピュータ100から出力される復号化情報読み込み信号がL（Low）レベルになると、選択部104は、選択指示保持部105に設定されている選択指示に基づいて、復号化部102の出力またはメモリ120の出力を選択的にCPU101に入力するように切り替わる。

【0047】

(S207) CPU101が実行ブロックの各命令コードに応じたアドレスを出力し、メモリ120から出力された命令コードは、選択部104を介し、暗号化の有無に応じて、すなわち暗号化されている場合には復号化部102により復号化された後、または平文である場合にはそのまま、CPU101に入力される。

【0048】

(S208) メモリ120から出力されたのが実行終了コード230であれば、（S202）に戻って次のデータブロックについて同じ処理が繰り返される

。(すなわち、鍵データ一時保持部106aおよび選択指示一時保持部106bに一旦保持された鍵データおよび選択指示が鍵データ保持部103および選択指示保持部105に設定されて、これらに基づいて次のデータブロックの読み込み等が行われる。)

(S209) 一方、メモリ120から出力されたのが実行終了コード230でなければ、CPU101は読み込まれた命令コードの命令を実行し、実行終了コード230が読み込まれるまで、(S207)～(S209)を繰り返す。

【0049】

上記のような動作が行われることにより、マイクロコンピュータ100に外部から与える必要のある鍵データは、最初に読み込まれるデータブロック201についての1つの鍵データだけなので、鍵データの管理の複雑化を招いたりすることがない一方、万一上記1つの鍵データが漏洩したとしても、その鍵データによって復号化できるのは最初のデータブロック201だけであり、他のデータブロックを復号化するための鍵データはそれぞれさらに他の鍵データによって暗号化されているので、メモリ120に記憶されている全てのデータが容易に知られてしまうことはない。すなわち、理論的には、1つの鍵データが知られてしまうと、それを基に復号化情報の復号化、次の鍵データの抽出を繰り返すことによって全てのデータを得ることは不可能ではないが、そのためには、暗号化アルゴリズムも知る必要があるとともに、実行ブロック221～225を解析するなどして、各データブロック201～205の区切りや読み込み順序等を判別する必要があるうえ、復号化情報211～215のフォーマットやデータブロック201～205内での位置（各データブロック201～205の先頭に配置されているとは限らない。）などを認識する必要があるので、メモリ120の記憶内容を解読することは相当に困難なものとなる。そして、その困難性が高いほど、解読に要する労力や費用、時間が増大するため、實際上、記憶内容の漏洩を防止することが容易にできる。

【0050】

上記のように記憶媒体に記憶された内容の秘匿性を高めることができるので、このような情報処理装置を例えばネットワークを介した通信を行う機器に適用す

ることによって、送受されるデータの暗号化処理や通信相手が正しいかどうかを確認する認証処理などを行うプログラム（アルゴリズムやプロトコル）が解読されるのを防止して、通信のセキュリティを確保することなども容易にできる。

【0051】

なお、前記の例では、実行ブロック221～225のうちの何れかについてだけ暗号化する例を示したが、これに限らず全て暗号化するようにしてもよい。その場合には、選択部104および選択指示保持部105や、復号化情報管理部106の選択指示一時保持部106b等は設けず、常にメモリ120の出力が復号化部102を介してCPU101に入力されるようにすることができ、また、復号化情報211～215に暗号化有無情報211b～215bを含めないようにすることもできる。それゆえ、マイクロコンピュータ100の構成の簡素化等を図ることができる。一方、前記の例のように一部の実行ブロックだけ暗号化する場合、すなわち、例えば規格化された手順の処理を行うプログラム（ルーチン）など、第三者に漏洩しても問題とならないような部分を暗号化しないようにする場合には、復号化に要する処理時間の影響を小さく抑えることが容易にできる。

【0052】

また、一部の実行ブロックについてだけ暗号化する場合、暗号化された実行ブロックを含むデータブロック（暗号化データブロック）にだけ、鍵データを含めるようにしてもよい。すなわち、暗号化データブロックに、その後に最初に読み込まれる暗号化データブロックの鍵データおよび実行ブロックを復号化する鍵データを含めるようにすれば、暗号化されない実行ブロックを含むデータブロックについては、鍵データを含めないようにでき、復号化部102による復号化動作も不要にすることができる。（なお、鍵データを含める必要がない場合でも、乱数を設定するなどして、復号化情報の長さが一定になるようにしたりしてもよい。）

また、各データブロックには、次のデータブロック（または次の暗号化データブロック）の鍵データと実行ブロックを復号化する鍵データを含める例を示したが、そのデータブロック自体に含まれる実行ブロックと、次のデータブロック（または次の暗号化データブロック）に含まれる鍵データとを復号化する鍵データ

を含めるようにしてもよい。すなわち、各データブロックに含まれる鍵データの読み込みが完了するまでは、鍵データ保持部 103 に保持された、以前のデータブロックの実行ブロックを復号化したのと同じ鍵データを用いて復号化し、その復号化が完了して実行ブロックの読み込みが開始される時点で、上記復号化された新たな鍵データが鍵データ保持部 103 に設定されて用いられるようにすればよい。また、このような場合などにおいて、新たな鍵データが復号化された直後に、その新たな鍵データが用いられる場合には、鍵データ一時保持部 106a や選択指示一時保持部 106b は必ずしも設けなくてもよい。

【0053】

(実施の形態 2)

上記実施の形態 1 のマイクロコンピュータは、データブロックの読み込み順序が一定であるような記憶内容を読み込むように構成されているのに対し、例えば条件分岐命令の実行などによって、あるデータブロックの次に読み込まれるデータブロックが必ずしも一定ではないような場合でも記憶内容を適切に読み込ませることができるマイクロコンピュータの例について説明する。すなわち、このマイクロコンピュータでは、データブロック中に含まれた、次に読み込む可能性がある全てのデータブロックについての鍵データを読み込んで保持しておくことにより、柔軟な順序でデータブロックを読み込むことができるようになっている。なお、以下の実施の形態において、前記実施の形態 1 等と同様の機能を有する構成要素等については同一の符号を付して説明を省略する。

【0054】

(装置の構成)

図 6 は本発明の実施の形態 2 のマイクロコンピュータ 300 の要部の構成とメモリ 120 を示すブロック図である。このマイクロコンピュータ 300 は、実施の形態 1 (図 1) のマイクロコンピュータ 100 と比べて、CPU 101、選択部 104、および復号化情報管理部 106 に代えて、CPU 301、選択部 304、および復号化情報管理部 306 を備えている点が異なっている。

【0055】

CPU 301 には、メモリ 120 に記憶されたデータブロックにおける復号化

情報の読み込み動作を制御する復号化制御部 301a が設けられている。この復号化制御部 301a と実施の形態 1 の復号化制御部 101a との相違は、後述するようにメモリ 120 に記憶されるデータブロックの形式が実施の形態 1 とは異なることに対応するものである。

【0056】

選択部 304 は、選択指示保持部 105 に設定された選択指示に応じてメモリ 120 または復号化部 102 の出力を選択する点は実施の形態 1 の選択部 104 と同じであるが、上記選択指示に係らず、例えば CPU 301 から入力されるデータブロック番号・鍵データ数読み込み信号が H レベルになった場合には、メモリ 120 の出力が直接選択される一方、鍵情報読み込み信号が H レベルになった場合には、復号化部 102 の出力が選択されるようになっている。

【0057】

復号化情報管理部 306 は、鍵テーブル 306a と制御部 306b とを備えている。上記鍵テーブル 306a は、CPU 301 から、鍵番号、鍵データ、および選択指示が入力されると、例えば図 7 に示すように、上記鍵番号と対応させて、鍵データと選択指示とを保持するようになっている。また、制御部 306b は、CPU 301 から入力されるデータブロック番号に基づいて、そのデータブロック番号に一致する鍵番号と対応して鍵テーブル 306a に保持されている鍵データと選択指示とを出力するようになっている。

【0058】

(メモリ 120 に記憶されるデータの形式)

また、メモリ 120 には、実施の形態 1 と同様に複数の（例えば 7 つの）データブロック 401～407 が記憶されているが、各データブロック 401～407 は、例えば図 8 に示すような構造を有している。すなわち、例えば主にデータブロック 401 を代表として説明すると、データブロック 401 には、データブロック番号 421、鍵データ数 431、および 1 つ以上の鍵情報 441 を含む復号化情報 411 と、実行ブロック 451 とが含まれている。各データブロック 401～407 の鍵情報 441～447 は全て暗号化される一方、実行ブロック 451～457 は必要に応じて（例えばデータブロック 401・402 の実行プロ

ック 4 5 1・4 5 2 だけが) 暗号化されている。

【0059】

上記復号化情報 4 1 1 のデータブロック番号 4 2 1 はデータブロックを特定するもので、データブロック 4 0 1 と一意に対応付けて設定されている。

【0060】

鍵データ数 4 3 1 は、復号化情報 4 1 1 中に含まれる鍵情報 4 4 1 の数（すなわち、後述するようにデータブロック 4 0 1 の次に読み込まれる可能性があるデータブロックの数）を示すもので、CPU 3 0 1 がデータブロック 4 0 1 中の全ての鍵情報 4 4 1 を読み込むために用いられる。なお、鍵データ数 4 3 1 を用いるのに代えて、復号化情報 4 1 1 の末尾に、復号化情報 4 1 1 の末尾であることを示す終了コードを設けて、鍵情報 4 4 1 の読み込み処理を完了させ得るようにしてもよい。

【0061】

鍵情報 4 4 1 は、データブロック 4 0 1 の次に CPU 3 0 1 に読み込まれる可能性がある 1 つ以上のデータブロックに対応して設けられ、それぞれ、鍵番号 4 4 1 a と、鍵データ 4 4 1 b と、暗号化有無情報 4 4 1 c とを含んでいる。具体的には、例えばデータブロック 4 0 1 の次に、後述するデータブロック分岐命令などによってデータブロック 4 0 2 の実行ブロック 4 5 2 またはデータブロック 4 0 3 の実行ブロック 4 5 3 が選択的に実行されるとし、前記のようにデータブロック 4 0 2 の実行ブロック 4 5 2 は暗号化される一方、データブロック 4 0 3 の実行ブロック 4 5 3 は暗号化されないとすると、復号化情報 4 1 1 には次のような 2 つの鍵情報 4 4 1 が設けられる。

【0062】

すなわち、一方の鍵情報 4 4 1 には、

(a) 鍵番号 4 4 1 a として、データブロック 4 0 2 のデータブロック番号 4 2 2 と等しい値が設定され、

(b) 鍵データ 4 4 1 b として、データブロック 4 0 2 の鍵情報 4 4 2 と実行ブロック 4 5 2 とを復号化するための鍵データが設定され、

(c) 暗号化有無情報 4 4 1 c として、実行ブロック 4 5 2 が暗号化されている

ことを示す値（例えば 0 x 1 0）が設定される。

【0063】

また、もう一方の鍵情報 4 4 1 には、

(a) 鍵番号 4 4 1 a として、データブロック 4 0 3 のデータブロック番号 4 2 3 と等しい値が設定され、

(b) 鍵データ 4 4 1 b として、データブロック 4 0 3 の鍵情報 4 4 3 を復号化するための鍵データが設定され、

(c) 暗号化有無情報 4 4 1 c として、実行ブロック 4 5 3 が暗号化されていないことを示す値（例えば 0 x 0 1）が設定される。

【0064】

なお、上記鍵情報 4 4 1 は、次に読み込まれる可能性があるデータブロックに対応するものだけでなく、例えば全てのデータブロックに対応するものを設けるようにして、後述するように鍵情報 4 4 1 を生成する際に、データブロックの読み込み順序の解析などをしなくてもよいようにしてもよい。

【0065】

また、データブロック 4 0 1 の実行ブロック 4 5 1 は、一連の命令コードから成るプログラム（データ）が分割された、他のデータブロックへのデータブロック分岐命令を含む命令コード列によって構成されている。上記データブロック分岐命令は、具体的には、例えば図 9 に示すように、条件分岐命令 5 0 1 の後に、データブロック 4 0 2 ・ 4 0 3 への無条件データブロック分岐命令 5 0 2 が設けられ、上記条件分岐命令 5 0 1 により判定条件に応じて分岐した後に、データブロック 4 0 2 ・ 4 0 3 の何れかに制御が移行するようになっている（言い換えれば、次に何れのデータブロックに移行するかはあらかじめ定まっておらず、何れに移行する可能性もある。）。また、条件判断によって、直接、データブロック 4 0 2 ・ 4 0 3 に移行する条件データブロック分岐命令 5 0 3 や、データブロック 4 0 1 の内外に移行する条件データブロック内外分岐命令 5 0 4 を用いたりしてもよい。

【0066】

上記のようなデータのメモリ 1 2 0 への格納は、例えば、前記実施の形態 1（

図4)と同じように、図10に示すようにして行うことができる。すなわち、図10における(S301)(S302)(S305)および(S306)は、実質的に図4の(S101)(S102)(S105)および(S106)とほぼ同じである。(S303)では、各データブロック401~407にデータブロック番号421~427を割り当てて一方、命令コード列を解析して、各データブロック401~407から分岐する可能性のあるデータブロックを求め、分岐先のデータブロックに応じた鍵番号441a~447aと鍵データ441b~447bと暗号化有無情報441c~447cとから鍵情報441~447を生成するとともに、上記割り当てられたデータブロック番号421~427、分岐先の数に等しい値の鍵データ数431~437、および鍵情報441~447を連結することにより、復号化情報411~417が生成される。また、(S304)では、各命令コード列に含まれる分岐命令のうち、他のデータブロックに分岐するものをデータブロック分岐命令に置換して実行ブロック451~457を生成し、これと復号化情報411~417とからデータブロック401~407が生成される。なお、上記のような分岐命令の置換を行わず、元のプログラムが生成される際に、あらかじめデータブロック分岐命令が用いられるようにしてもよい。

【0067】

(メモリ120に記憶されたデータの読み込みと実行動作)

上記のようにメモリ120に記憶されたプログラムがマイクロコンピュータ300に読み込まれて実行される場合の動作について、図11に基づいて説明する。

【0068】

(S401) マイクロコンピュータ300の外部から、最初に読み込まれるデータブロック、例えばデータブロック401についての鍵データ440bと、その鍵データ440bがデータブロック401に対するものであることを示す鍵番号440a(すなわちデータブロック401のデータブロック番号421に等しい値)と、暗号化された実行ブロック451が読み込まれる際に選択部304によって復号化部102の出力を選択することを示す選択指示とが入力されると

、これらを復号化情報管理部 3 0 6 の鍵テーブル 3 0 6 a が保持する。

【 0 0 6 9 】

(S 4 0 2) 復号化制御部 3 0 1 a の制御によって、C P U 3 0 1 が選択部 3 0 4 に例えば H レベルのデータブロック番号・鍵データ数読み込み信号を出力すると、選択部 3 0 4 は、選択指示保持部 1 0 5 から出力される選択指示に係らず、メモリ 1 2 0 からの出力を直接選択するように切り替わる。

【 0 0 7 0 】

(S 4 0 3) 復号化制御部 3 0 1 a の制御によって、C P U 3 0 1 が復号化情報におけるデータブロック番号と鍵データ数とを読み込むためのアドレス（および図示しない読み出し制御信号）を順次メモリ 1 2 0 に出力する。これに応じて、メモリ 1 2 0 はデータブロック番号と鍵データ数とを出力する。このデータブロック番号と鍵データ数とは、そのまま（復号化部 1 0 2 による復号化がなされることなく）選択部 3 0 4 を介して C P U 3 0 1 に入力される。

【 0 0 7 1 】

(S 4 0 4) C P U 3 0 1 が上記データブロック番号を（図示しない出力タイミング信号と共に）復号化情報管理部 3 0 6 に出力すると、制御部 3 0 6 b は、鍵テーブル 3 0 6 a に保持された鍵番号のうち、上記データブロック番号に一致する鍵番号と対応して保持されている鍵データおよび選択指示をそれぞれ鍵データ保持部 1 0 3 または選択指示保持部 1 0 5 に出力して設定する。ここで、上記データブロック番号と鍵テーブル 3 0 6 a に保持されている各鍵番号とが一致するかどうかの判定は、例えば、各鍵番号について並列に行わせるようにしてもよいし、一致するものが検出されるまで順次比較を行わせるようにしてもよい。ただし、特に後者の場合に、検出に要する時間が不定となる場合には、検出されたことを示す検出信号や鍵データ保持部 1 0 3 および選択指示保持部 1 0 5 への設定が完了したことを示す設定終了信号を C P U 3 0 1 に出力する一方、C P U 3 0 1 は上記信号が入力されるまで鍵情報 4 4 1 の読み込み（アドレスの出力等）を開始しないようにすることが好ましい。

【 0 0 7 2 】

(S 4 0 5) C P U 3 0 1 がデータブロック番号・鍵データ数読み込み信号

を L レベル、鍵情報読み込み信号を H レベルにし、選択部 3 0 4 は復号化部 1 0 2 の出力を選択するように切り替わる。

【 0 0 7 3 】

(S 4 0 6) CPU 3 0 1 が上記鍵データ数に応じた数の鍵情報を順次メモリ 1 2 0 から選択部 3 0 4 を介して読み込み、鍵番号と、鍵データと、暗号化有無情報に応じた選択指示とを（図示しない出力タイミング信号と共に）復号化情報管理部 3 0 6 に出力して、鍵テーブル 3 0 6 a に保持させる。

【 0 0 7 4 】

(S 4 0 7) 鍵データ数に応じた数の鍵情報についての処理が完了すると、CPU 3 0 1 は鍵情報読み込み信号を L レベルにする。そこで、選択部 3 0 4 は、選択指示保持部 1 0 5 に設定されている選択指示に基づいて、復号化部 1 0 2 の出力またはメモリ 1 2 0 の出力を選択的に CPU 3 0 1 に入力するように切り替わる。

【 0 0 7 5 】

(S 4 0 8) CPU 3 0 1 が実行ブロックの各命令コードに応じたアドレスを出力し、メモリ 1 2 0 から出力された命令コードは、選択部 3 0 4 を介し、暗号化の有無に応じて、すなわち暗号化されている場合には復号化部 1 0 2 により復号化された後、または平文である場合にはそのまま、CPU 3 0 1 に入力される。

【 0 0 7 6 】

(S 4 0 9) CPU 3 0 1 に入力された命令コードの命令がデータブロック分岐命令であれば、(S 4 0 2) に戻って次のデータブロックについて同じ処理が繰り返される。

【 0 0 7 7 】

(S 4 1 0) 一方、データブロック分岐命令でなければ、CPU 3 0 1 は読み込まれた命令コードの命令を実行し、データブロック分岐命令が読み込まれるまで、(S 4 0 8) ～ (S 4 1 0) を繰り返す。

【 0 0 7 8 】

上記のように、各データブロックに分岐先のデータブロックに応じた 1 つ以上

の鍵データを含めることにより、データブロックの読み込み順序が一定でない場合でも適切に各データブロックの内容を読み込むことができるので、実施の形態 1 と同様に記憶内容の秘匿性を高められることに加えて、プログラムの作成や分割を柔軟に行うことが容易にできる。

【0079】

なお、上記のように各データブロックに、分岐先となる可能性のあるデータブロック用の鍵データを（暗号化して）含めるのに代えて、分岐先となるデータブロックに、そのデータブロック用の複数の同一の鍵データが、それぞれ、そのデータブロックに分岐してくる分岐元となる可能性のあるデータブロックと同じように暗号化されたものを含めるようにしてもよい。すなわち、分岐先のデータブロックで読み込まれた複数の暗号化された鍵データのうち、分岐元のデータブロックに対応するものが、分岐元のデータブロックと同じ鍵データを用いて復号化されるようにすれば、そのデータブロック用の適切な鍵データを得ることができる。

【0080】

（実施の形態 3）

上記実施の形態 2 と同様に、任意の順序でデータブロックを読み込ませることができるマイクロコンピュータの他の例について説明する。

【0081】

（メモリ 120 に記憶されるデータの形式）

まず、このマイクロコンピュータで読み込まれるデータがメモリ 120 に記憶される形式について、図 12 に基づいて説明する。メモリ 120 には、複数の（例えば 3 つの）データブロック 701～703 が記憶され、各データブロック 701～703 は、復号化情報 711'～713' と、実行ブロック 721～723 とから構成されている。上記実行ブロック 721～723 は、実施の形態 1 と同様に、一連の命令コードから成るプログラム（データ）が 3 つの実行単位に分割された命令コード列 721a～723a に実行終了コード 230 が付加されて構成され、必要に応じて（例えば実行ブロック 721 が）暗号化されている。

【0082】

上記暗号化された実行ブロック 721 を含むデータブロック 701 の復号化情報 711' は、上記実行ブロック 721 を復号化するための鍵データ 711 が所定の共通鍵データ 740 により暗号化されたものである。一方、暗号化されていない実行ブロック 722・723 を含むデータブロック 702・703 の復号化情報 712'・713' は、所定のダミー鍵データ 710 が、データブロック 701 と同じ共通鍵データ 740 により暗号化されたものである。（なお、復号化情報 711'～713' には、前記実施の形態 1、2 のように暗号化有無情報は含まれていないが、この点については後述する。）上記共通鍵データ 740 は、特に限定されないが、システムごとに異なせると、データの秘匿性をより高めることが容易にできる。また、上記共通鍵データ 740 による鍵データ 711 の暗号化の手法も、実行ブロック 721 と同様に、共通鍵暗号方式など種々の手法を適用することができる。

【0083】

（装置の構成）

上記のような記憶内容を読み込むマイクロコンピュータ 600 は、図 13 に示すように、実施の形態 1（図 1）のマイクロコンピュータ 100 と比べて、CPU 101、選択部 104、および復号化情報管理部 106 に代えて、CPU 601、選択部 604、および復号化情報管理部 606 を備えている点が異なっている。

【0084】

CPU 601 に設けられる復号化制御部 601a と実施の形態 1 の復号化制御部 101a との相違は、上記のようにメモリ 120 に記憶されるデータブロックの形式が実施の形態 1 とは異なることに対応するものである。

【0085】

選択部 604 は、例えば H レベルの復号化情報読み込み信号が入力される場合には、選択指示保持部 105 に設定された選択指示に係らず、メモリ 120 の出力を選択するようになっている。

【0086】

復号化情報管理部 606 は、鍵データ復号化部 606a（第 2 の復号化部）と

、共通鍵データ保持部 6 0 6 b（第 2 の鍵データ保持部）と、暗号化有無判定部 6 0 6 c と、比較データ保持部 6 0 6 d とを備えている。

【0 0 8 7】

鍵データ復号化部 6 0 6 a は、CPU 6 0 1 がメモリ 1 2 0 から読み込んで出力した復号化情報 7 1 1' ～ 7 1 3'（暗号化された鍵データ 7 1 1 またはダミー鍵データ 7 1 0）を復号化して、元の鍵データ 7 1 1 またはダミー鍵データ 7 1 0 を出力するようになっている。上記鍵データの復号化には、マイクロコンピュータ 6 0 0 の外部から入力されて共通鍵データ保持部 6 0 6 b に保持された共通鍵データ 7 4 0 が用いられる。

【0 0 8 8】

暗号化有無判定部 6 0 6 c は、上記鍵データ復号化部 6 0 6 a の出力と、マイクロコンピュータ 6 0 0 の外部から入力されて比較データ保持部 6 0 6 d に保持されたダミー鍵データ 7 1 0 とを比較し、一致する場合には、選択部 6 0 4 にメモリ 1 2 0 からの出力を選択させる選択指示を出力する一方、一致しない場合には、復号化部 1 0 2（第 1 の復号化部）からの出力を選択させる選択指示を出力するようになっている。すなわち、実行ブロック 7 2 2・7 2 3 が暗号化されていないデータブロック 7 0 2・7 0 3 の復号化情報 7 1 2'・7 1 3' が復号化されると鍵データ復号化部 6 0 6 a からはダミー鍵データ 7 1 0 が出力されるので、これと、比較データ保持部 6 0 6 d に保持されているダミー鍵データ 7 1 0 とが一致すると判定されることによって、実行ブロック 7 2 2・7 2 3 が暗号化されていないことを判別でき、選択部 6 0 4 にメモリ 1 2 0 の出力を選択させることができる。（なお、この場合、鍵データ保持部 1 0 3（第 1 の鍵データ保持部）に上記ダミー鍵データ 7 1 0 が保持されたとしても、復号化部 1 0 2 の出力は選択部 6 0 4 によって選択されないため、CPU 6 0 1 に入力されるデータには影響がない。）

前記のようなデータのメモリ 1 2 0 への格納は、例えば図 1 4 に示すようにして行うことができる。同図において、（S 5 0 2）（S 5 0 5）（S 5 0 7）は、実質的に前記実施の形態 1（図 4）の（S 1 0 1）（S 1 0 4）（S 1 0 6）とほぼ同じである。（S 5 0 1）では、データブロック 7 0 1～7 0 3 の復号化

情報 711' ~ 713' を復号化して鍵データ 711 またはダミー鍵データ 710 を得るための共通鍵データ 740 を決定し、(S503) では、データブロック 701 用の鍵データ 711 を決めるとともにデータブロック 702・703 用のダミー鍵データ 710 を決め、(S504) では、鍵データ 711 およびダミー鍵データ 710 が共通鍵データ 740 で暗号化されて復号化情報 711' ~ 713' が得られる。また、(S506) では、実行ブロック 721 だけが鍵データ 711 によって暗号化される。

【0089】

(メモリ 120 に記憶されたデータの読み込みと実行動作)

上記のようにメモリ 120 に記憶されたプログラムがマイクロコンピュータ 600 に読み込まれて実行される場合の動作について、図 15 に基づいて説明する。

【0090】

(S601) マイクロコンピュータ 600 の外部から、共通鍵データ 740、およびダミー鍵データ 710 が入力されると、これらを復号化情報管理部 606 の共通鍵データ保持部 606b、および比較データ保持部 606d が保持する。

【0091】

(S602) 復号化制御部 601a の制御によって、CPU 601 が選択部 604 に例えば H レベルの復号化情報読み込み信号を出力すると、選択部 604 は、選択指示保持部 105 から出力される選択指示に係らず、メモリ 120 からの出力を直接選択するように切り替わる。

【0092】

(S603) 復号化制御部 601a の制御によって、CPU 601 がメモリ 120 に復号化情報を読み込むためのアドレス（および図示しない読み出し制御信号）を出力する。これに応じて、メモリ 120 は復号化情報を出力する。この復号化情報は、そのまま（復号化部 102 による復号化がなされることなく）選択部 604 を介して CPU 601 に入力される。ここで、復号化情報が復号化部 102 によって復号化されないのは、後に鍵データ復号化部 606a によって復

号化されるからである。

【0093】

(S604) CPU601は、入力された復号化情報を復号化情報管理部606の鍵データ復号化部606aに(図示しない出力タイミング信号と共に)出力する。

【0094】

(S605) 鍵データ復号化部606aが、共通鍵データ保持部606bに保持されている共通鍵データ740を用いて、CPU601から入力された復号化情報を復号化し、得られた鍵データ711(またはダミー鍵データ710)を鍵データ保持部103に設定するとともに、暗号化有無判定部606cにも出力する。

【0095】

(S606) 暗号化有無判定部606cは鍵データ復号化部606aの出力と比較データ保持部606dに保持されているダミー鍵データ710と比較し、一致する場合には、選択部604にメモリ120からの出力を選択させる選択指示を出力する一方、一致しない場合には、復号化部102からの出力を選択させる選択指示を出力して、選択指示保持部105に設定する。すなわち、鍵データ復号化部606aによって復号化されたのがダミー鍵データ710であれば、そのデータブロックの実行ブロックは暗号化されていないので、選択部604にメモリ120からの出力を選択させ、そのままCPU601に入力させるようにする。また、鍵データ復号化部606aによって復号化されたのがダミー鍵データ710でなければ、それは鍵データなので、選択部604に復号化部102の出力を選択させ、上記(S605)で鍵データ保持部103に設定された鍵データ711を用いて復号化されたデータをCPU601に入力させるようにする。

【0096】

(S607) CPU601から出力される復号化情報読み込み信号がLレベルになると、選択部604は、選択指示保持部105に設定されている選択指示に基づいて、復号化部102の出力またはメモリ120の出力を選択的にCPU601に入力するように切り替わる。

【0 0 9 7】

(S 6 0 8) CPU 6 0 1 が実行ブロックの各命令コードに応じたアドレスを出力し、メモリ 1 2 0 から出力された命令コードは、選択部 6 0 4 を介し、暗号化の有無に応じて、すなわち暗号化されている場合には復号化部 1 0 2 により復号化された後、または平文である場合にはそのまま、CPU 6 0 1 に入力される。

【0 0 9 8】

(S 6 0 9) メモリ 1 2 0 から出力されたのが実行終了コード 2 3 0 であれば、(S 6 0 2) に戻って次のデータブロックについて同じ処理が繰り返される。

【0 0 9 9】

(S 6 1 0) 一方、メモリ 1 2 0 から出力されたのが実行終了コード 2 3 0 でなければ、CPU 6 0 1 は読み込まれた命令コードの命令を実行し、実行終了コード 2 3 0 が読み込まれるまで、(S 6 0 8) ~ (S 6 1 0) を繰り返す。

【0 1 0 0】

上記のように、各実行ブロックを復号化する鍵データを、各実行ブロックと同じデータブロックに含めることにより、上記鍵データの取得はデータブロックの読み込み順序に依存しないので、任意の順序で読み込むことができる。また、マイクロコンピュータ 6 0 0 の外部から与える必要のある（管理する必要のある）鍵データは、（各実行ブロックを復号化するための鍵データを復号化する）上記共通鍵データだけなので、やはり、鍵データの管理の簡素化を図ることができる。ここで、上記共通鍵データが万一漏洩すると複数の鍵データが解読される可能性はあるが、これによって知られてしまうのはあくまで鍵データだけであり、記憶データを取得するためには、さらにその鍵データを用いた復号化を行わなければならない。そして、そのためには、鍵データの他に暗号化アルゴリズム、各データブロック 7 0 1 ~ 7 0 3 の区切りや復号化情報 7 1 1' ~ 7 1 3' と実行ブロック 7 2 1 との区切り、復号化情報 7 1 1' ~ 7 1 3' の配置なども知る必要があるので、メモリ 1 2 0 の記憶内容を解読することはやはり非常に困難であり、實際上、記憶内容の漏洩を防止することが容易にできる。

【0101】

なお、上記の例では、暗号化有無判定部606cが鍵データ復号化部606aの出力を比較データ保持部606dの出力と比較する例を示したが、鍵データ保持部103の出力を比較するようにしてもよい。この場合には、鍵データ保持部103に同じ値が保持されている間は、暗号化有無判定部606cからの出力も同じに保たれるので、選択指示保持部105を省略することができる。

【0102】

さらに、CPU601から出力される（鍵データ復号化部606aによる復号化前の）復号化情報711'～713'を比較データ保持部606dの出力と比較するようにしてもよい。この場合には、データブロック701～703の復号化情報712'・713'を生成する際にダミー鍵データ710を暗号化しなくてもよい。

【0103】

また、上記の例では、復号化情報711'～713'の復号化を鍵データ復号化部606aが行い、実行ブロック721～723の復号化を復号化部102が行うように構成された例を示したが、これに限らず、例えばそれぞれの復号化を行う際に、共通鍵データ740または鍵データ711を鍵データ保持部103に設定するようにして、何れの復号化も復号化部102によって行わせるようにしてもよい。このように復号化部を兼用することによりハードウェア規模を小さく抑えることができる。一方、前記のように復号化部を分けて設ける場合には、兼用する場合に比べて、それぞれの復号化に互いに異なるアルゴリズムを用いるようにすることが容易にできる。特に、鍵データの復号化は各データブロックについて1回行うだけなので、マイクロコンピュータ600の処理時間に大きな影響を与えることなく、暗号強度の高い暗号化方式を適用することなども容易にできる。

【0104】

ここで、例えば、鍵データ復号化部606aの復号化に要するクロックサイクルが、ループ処理などによって複数クロックになる場合や不定である場合には、鍵データ復号化部606aによる復号化が完了して鍵データ保持部103に

鍵データが設定されるタイミングで復号化情報管理部606から設定終了信号を出力させ、これがCPU601に入力されるまでの間、CPU601に次のアドレス出力等のデータの読み込み動作を停止させるようにすれば、復号化部102によって復号化されたデータを確実にCPU601に入力させることが容易にできる。

【0105】

(実施の形態4)

上記実施の形態3の変形例で説明したようにCPU601がメモリ120から読み込んだ復号化情報711'～713'を鍵データ復号化部606aに出力した後、鍵データ復号化部606aによる復号化が完了して鍵データ711が鍵データ保持部103に設定されるまでの間にCPU601の動作を停止させる場合、マイクロコンピュータ300とメモリ120との間で送受される信号を監視すれば、マイクロコンピュータ600が通常のメモリアクセスをしている場合とは異なる動作をしていると推測しやすくなる。そこで、もし、メモリ120の記憶内容を不正に取得しようとする者によって、アドレスが出力されない期間にCPU601の内部で復号化処理がなされていると推測されたとすると、その直前に出力されたアドレスの領域に着目されやすくなる。その場合でも、その着目された領域に鍵データが記憶されているとは限らず、また、前記のように暗号化アルゴリズム等が判らなければ、メモリ120の記憶内容の解読は困難であることには変わりないが、上記のように特定の領域に着目されるようなことも起こりにくいようにするために、疑似的なアドレスをマイクロコンピュータ600から出力させるようにしてもよい。

【0106】

具体的には、例えば図16に示すマイクロコンピュータ800は、実施の形態3のマイクロコンピュータ600(図13)と比べて、CPU601と、復号化情報管理部606とに代えて、CPU601'と、鍵データ復号化部606a'を有する復号化情報管理部606'とを備えるとともに、さらに、疑似アドレス発生部811(疑似読み込み信号出力部)を備えている点が異なっている。

【0107】

上記鍵データ復号化部 6 0 6 a' は、復号化が完了して鍵データ保持部 1 0 3 に鍵データが設定されるタイミングで、例えば H レベルの設定終了信号を CPU 6 0 1' に出力するようになっている。

【 0 1 0 8 】

CPU 6 0 1' は、基本的な動作は CPU 6 0 1 と同じであるが、復号化情報管理部 6 0 6' の鍵データ復号化部 6 0 6 a' によって、暗号化された鍵データが復号化される間（すなわち、復号化情報 7 1 1' ～ 7 1 3' と伴に例えば H レベルの出力タイミング信号を鍵データ復号化部 6 0 6 a' に出力してから、H レベルの設定終了信号が鍵データ復号化部 6 0 6 a' から CPU 6 0 1' に入力されるまでの間）、次のアドレス出力等のデータの読み込み動作を停止するようになっている。

【 0 1 0 9 】

擬似アドレス発生部 8 1 1 は、CPU 6 0 1' から出力される復号化情報 7 1 1' ～ 7 1 3' の出力タイミング信号が H レベルになってから、鍵データ復号化部 6 0 6 a' から出力される設定終了信号が H レベルになるまでの間に、疑似的なアドレスを出力するようになっている。より詳しくは、CPU 6 0 1' から出力される出力タイミング信号が H レベルになると、乱数生成部 8 1 1 a は乱数を発生してインクリメント部 8 1 1 b に初期値として設定し（保持させ）、インクリメント部 8 1 1 b は、図示しないクロック信号に応じて、保持している値を順次インクリメントし、擬似アドレスとして出力するようになっている。また、出力制御部 8 1 1 c は、上記出力タイミング信号が H レベルになってから、設定終了信号が H レベルになるまでの間は、上記インクリメント部 8 1 1 b から出力される値（および図示しない読み出し制御信号）を出力する一方、その他の場合には、CPU 6 0 1' から出力されるアドレスをそのまま出力するようになっている。（上記のように擬似アドレスが出力されると、メモリ 1 2 0 からは無効なデータが出力されることになるが、その際、CPU 6 0 1' は上記のようにデータの読み込み動作を停止しているので、そのような無効なデータは CPU 6 0 1' に取り込まれない。）

なお、上記各実施の形態では、メモリ 1 2 0 の記憶内容がプログラムである例

を示したが、これに限らず、所定のプログラム（読み込みプログラム）の実行によって読み込まれる単なるデータなどが、同様に分割、暗号化されて記憶されるようにしてもよい。その場合、各データブロックの読み込み順序は、上記読み込みプログラムによってあらかじめ定められていてもよいし、データブロック中に含まれたポインタや管理情報などによって制御されるようにしてもよい。すなわち、何れの場合でも、どのデータブロックの次にどのデータブロックが読み込まれるかが定まってい、それに応じた鍵データが各データブロックに含まれるなどされていればよい。ここで、上記のように単なるデータが暗号化されて記憶されている場合、これを読み込む読み込みプログラムも同様に暗号化すれば、より秘匿性を高くすることができるが、読み込みプログラムを暗号化しなくても、これによって読み込まれる内容自体の解読は、やはり相当に困難なものにすることができる。

【0110】

また、上記の例では、鍵データ保持部103に設定される鍵データなどの初期値がマイクロコンピュータ100の外部から入力される例を示したが、これに限らずマイクロコンピュータ100の内部にあらかじめ設定された値などが用いられるようにしてもよい。

【0111】

また、図3等にしたデータ構造は論理的なもので、必ずしもメモリ120における物理的な記憶領域の関係が同図に示すようになっている必要はない。

【0112】

また、上記各実施の形態や変形例で説明した構成要素等は、それぞれ論理的に可能な範囲で、種々組み合わせてもよい。具体的には、例えば、実施の形態2～4において、実施の形態1の変形例で説明したように、選択部を設けず、全ての実行ブロックが暗号化されたデータブロックを読み込むようにしたり、実施の形態1、2において、選択部の切り替えを暗号化有無情報に基づいて行うのに代えて、実施の形態3、4で説明したようにダミー鍵データを用いて行うようにしたり、または逆に、実施の形態3、4において暗号化有無情報に基づいて切り替えるようにしたり、また、実施の形態1、2において、各復号化情報に含まれる鍵

データが実施の形態 3、4 と同様に共通鍵データによって復号化されるようにしたりしてもよい。

【0113】

【発明の効果】

以上のように本発明によると、記憶媒体に記憶されるべきデータを複数に分割して、それぞれ互いに異なる鍵データによって復号化されるように暗号化するとともに、上記鍵データも、それぞれ他の鍵データによって復号化されるように暗号化して記憶媒体に記憶させ、その記憶内容を読み込む際に、暗号化された鍵データから復号化された鍵データを用いて、暗号化されたデータおよび次の鍵データの復号化を順次行うようにすることにより、第三者が記憶媒体の記憶内容を不正に取得することの困難性を高めることができるとともに、複数の鍵データを管理する必要がなく、したがって、暗号鍵の管理の複雑化などを招くことなく、記憶媒体に記憶されたデータが容易に第三者に漏洩するのを防止可能にすることができる。

【図面の簡単な説明】

【図 1】

実施の形態 1 のマイクロコンピュータ 100 の要部の構成を示すブロック図である。

【図 2】

同、メモリ 120 の記憶内容の例を示す説明図である。

【図 3】

同、データブロック 201 のデータ構造の例を示す説明図である。

【図 4】

同、メモリ 120 へのデータの格納手順の例を示すフローチャートである。

【図 5】

同、メモリ 120 に記憶されたプログラムがマイクロコンピュータ 100 に読み込まれて実行される場合の動作を示すフローチャートである。

【図 6】

実施の形態 2 のマイクロコンピュータ 300 の要部の構成を示すブロック図で

ある。

【図 7】

同、鍵テーブル 3 0 6 a の保持内容の例を示す説明図である。

【図 8】

同、データブロック 4 0 1 のデータ構造の例を示す説明図である。

【図 9】

同、命令コード列中のデータブロック分岐命令の例を示す説明図である。

【図 1 0】

同、メモリ 1 2 0 へのデータの格納手順の例を示すフローチャートである。

【図 1 1】

同、メモリ 1 2 0 に記憶されたプログラムがマイクロコンピュータ 3 0 0 に読み込まれて実行される場合の動作を示すフローチャートである。

【図 1 2】

実施の形態 3 のデータブロック 7 0 1 のデータ構造の例を示す説明図である。

【図 1 3】

同、マイクロコンピュータ 6 0 0 の要部の構成を示すブロック図である。

【図 1 4】

同、メモリ 1 2 0 へのデータの格納手順の例を示すフローチャートである。

【図 1 5】

同、メモリ 1 2 0 に記憶されたプログラムがマイクロコンピュータ 6 0 0 に読み込まれて実行される場合の動作を示すフローチャートである。

【図 1 6】

実施の形態 4 のマイクロコンピュータ 8 0 0 の要部の構成を示すブロック図である。

【符号の説明】

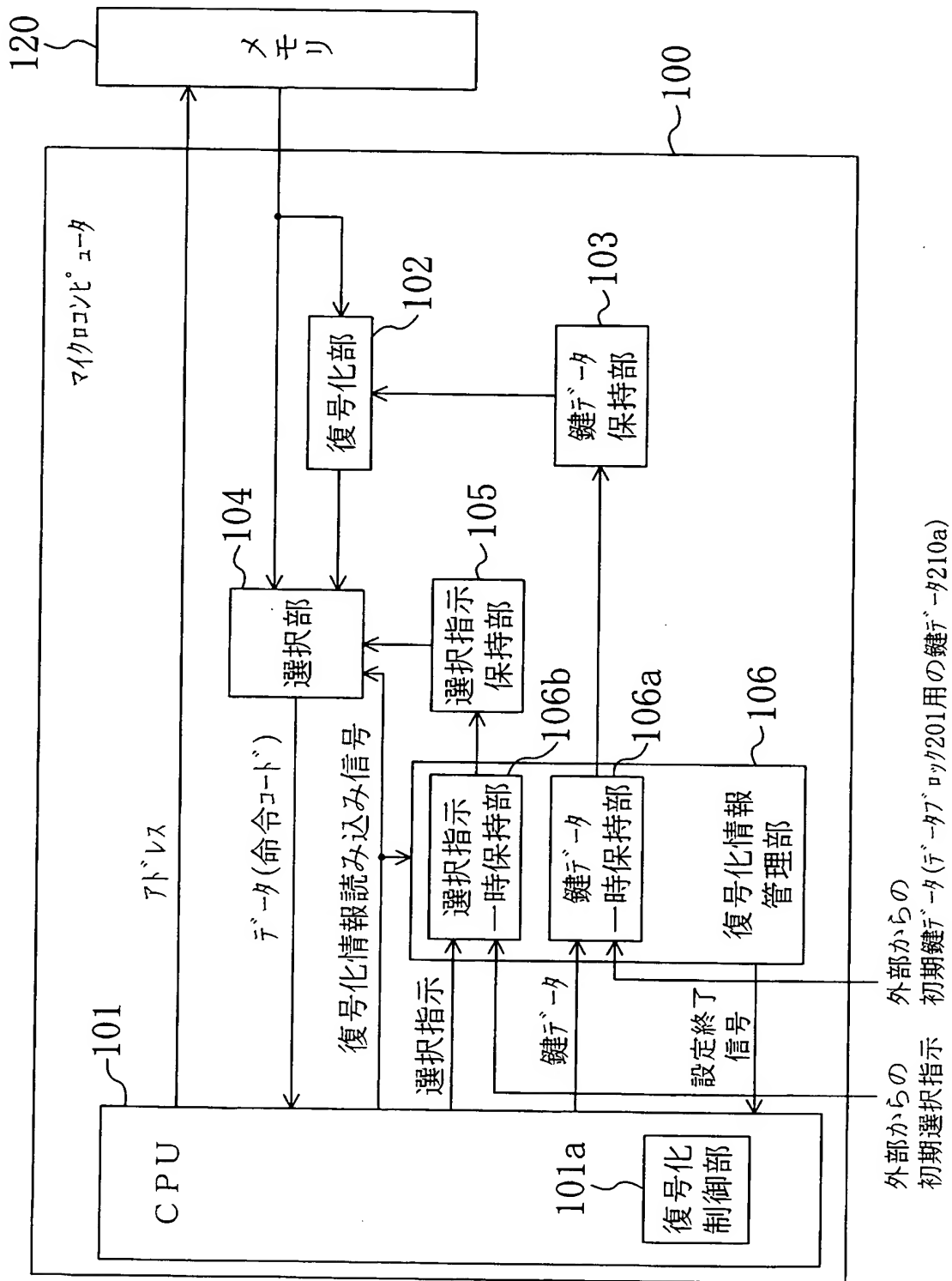
1 0 0	マイクロコンピュータ
1 0 1	C P U
1 0 1 a	復号化制御部
1 0 2	復号化部

1 0 3	鍵データ保持部
1 0 4	選択部
1 0 5	選択指示保持部
1 0 6	復号化情報管理部
1 0 6 a	鍵データ一時保持部
1 0 6 b	選択指示一時保持部
1 2 0	メモリ
2 0 1 ~ 2 0 5	データブロック
2 1 1 ~ 2 1 5	復号化情報
2 1 0 a ~ 2 1 5 a	鍵データ
2 1 1 b ~ 2 1 5 b	暗号化有無情報
2 2 1 ~ 2 2 5	実行ブロック
2 2 1 a ~ 2 2 5 a	命令コード列
2 3 0	実行終了コード
3 0 0	マイクロコンピュータ
3 0 1	C P U
3 0 1 a	復号化制御部
3 0 4	選択部
3 0 6	復号化情報管理部
3 0 6 a	鍵テーブル
3 0 6 b	制御部
4 0 1 ~ 4 0 7	データブロック
4 1 1 ~ 4 1 7	復号化情報
4 2 1 ~ 4 2 7	データブロック番号
4 3 1 ~ 4 3 7	鍵データ数
4 4 1 ~ 4 4 7	鍵情報
4 4 0 a ~ 4 4 7 a	鍵番号
4 4 0 b ~ 4 4 7 b	鍵データ
4 4 1 c ~ 4 4 7 c	暗号化有無情報

4 5 1 ~ 4 5 7	実行ブロック
5 0 1	条件分岐命令
5 0 2	無条件データブロック分岐命令
5 0 3	条件データブロック分岐命令
5 0 4	条件データブロック内外分岐命令
6 0 0	マイクロコンピュータ
6 0 1	C P U
6 0 1'	C P U
6 0 1 a	復号化制御部
6 0 4	選択部
6 0 6	復号化情報管理部
6 0 6'	復号化情報管理部
6 0 6 a	鍵データ復号化部
6 0 6 a'	鍵データ復号化部
6 0 6 b	共通鍵データ保持部
6 0 6 c	暗号化有無判定部
6 0 6 d	比較データ保持部
7 0 1 ~ 7 0 3	データブロック
7 1 0	ダミー鍵データ
7 1 1	鍵データ
7 1 1' ~ 7 1 3'	復号化情報
7 2 1 ~ 7 2 3	実行ブロック
7 2 1 a ~ 7 2 3 a	命令コード列
7 4 0	共通鍵データ
8 0 0	マイクロコンピュータ
8 1 1	擬似アドレス発生部
8 1 1 a	乱数生成部
8 1 1 b	インクリメント部
8 1 1 c	出力制御部

【書類名】 図面

【図 1】

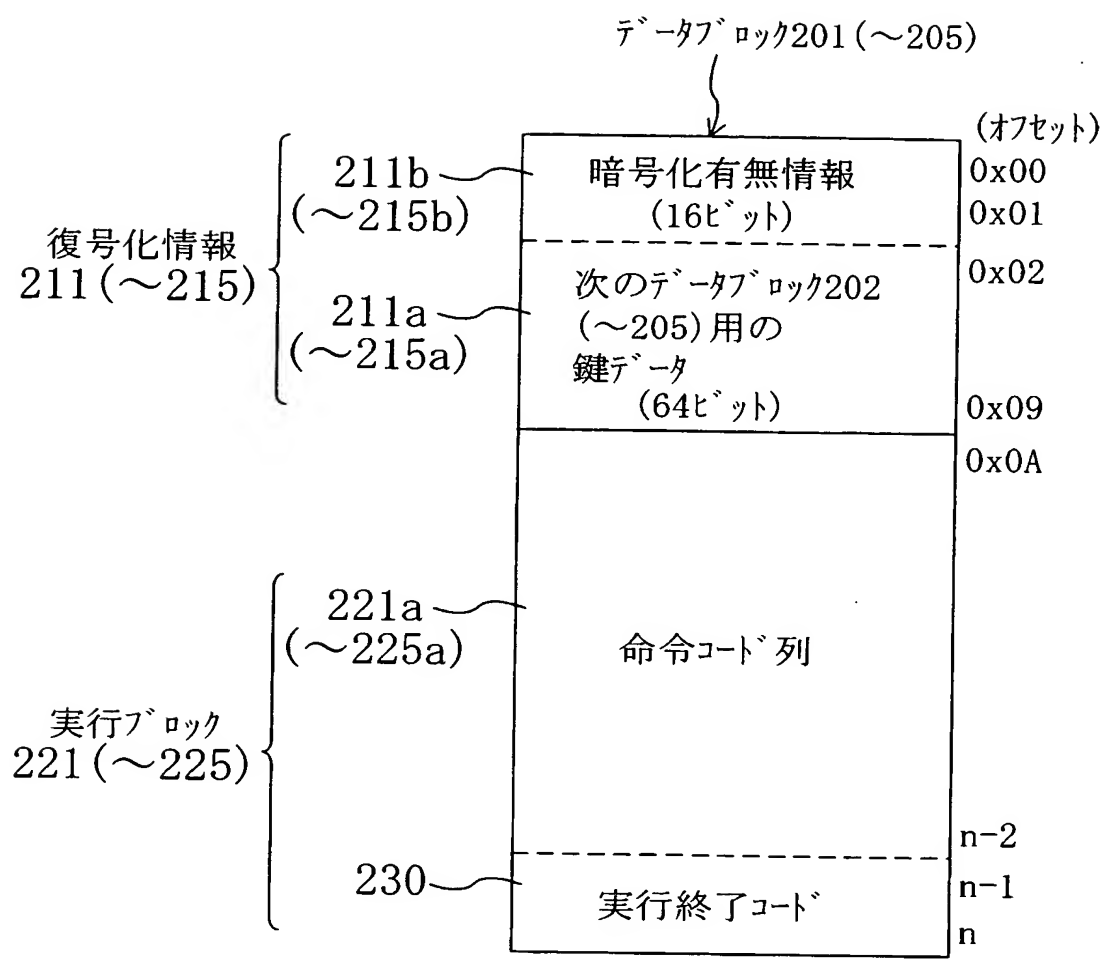


【図 2】

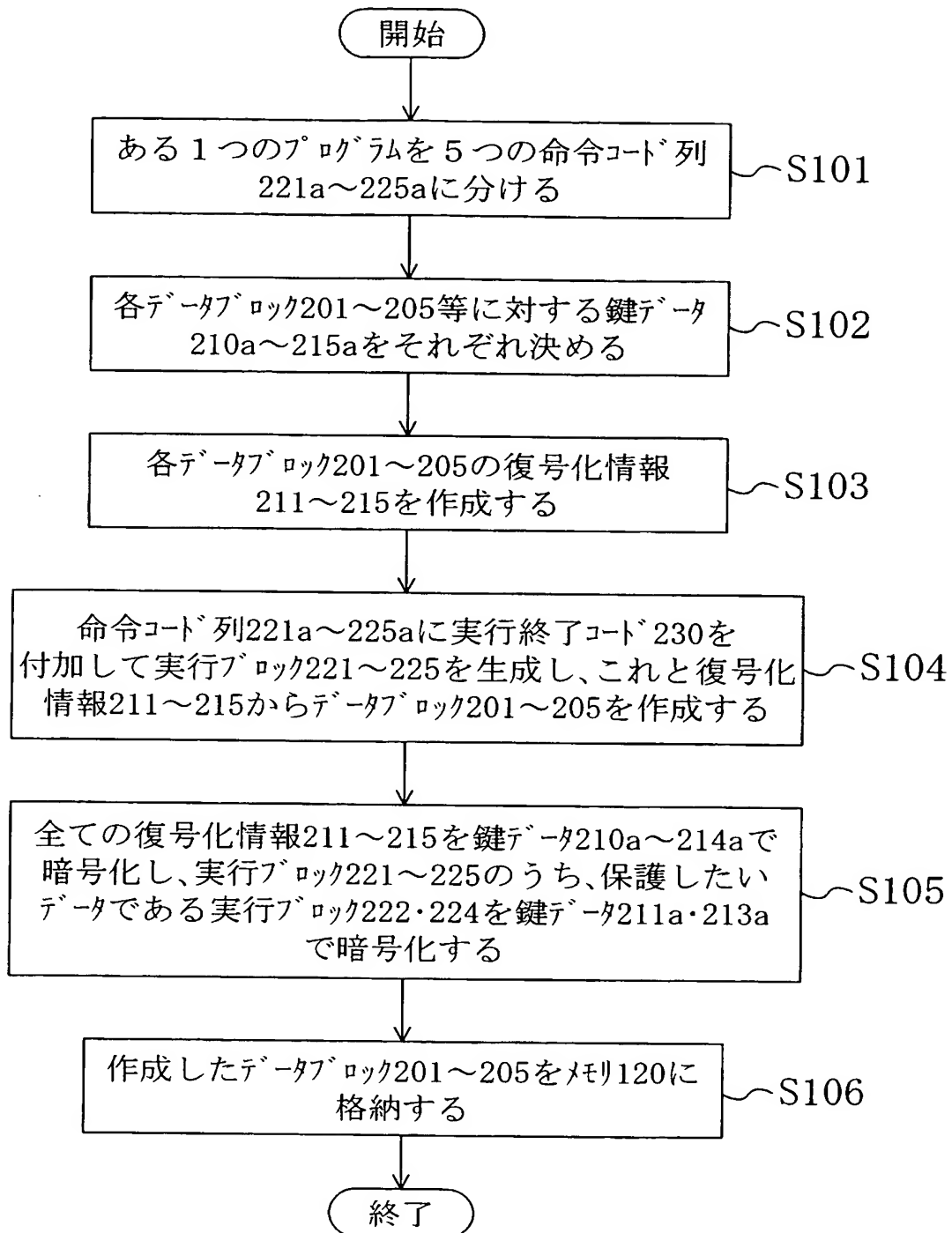
メモリ120の記憶内容

(アドレス)	
復号化情報211と平文の 実行ブロック221を含む データブロック	0x000000 〜 201
復号化情報212と暗号化 された実行ブロック222を 含むデータブロック	0x111110 0x111111 〜 202
復号化情報213と平文の 実行ブロック223を含む データブロック	0x222221 0x222222 〜 203
復号化情報214と暗号化 された実行ブロック224を 含むデータブロック	0x333332 0x333333 〜 204
復号化情報215と平文の 実行ブロック225を含む データブロック	0x444443 0x444444 〜 205 0xFFFFF

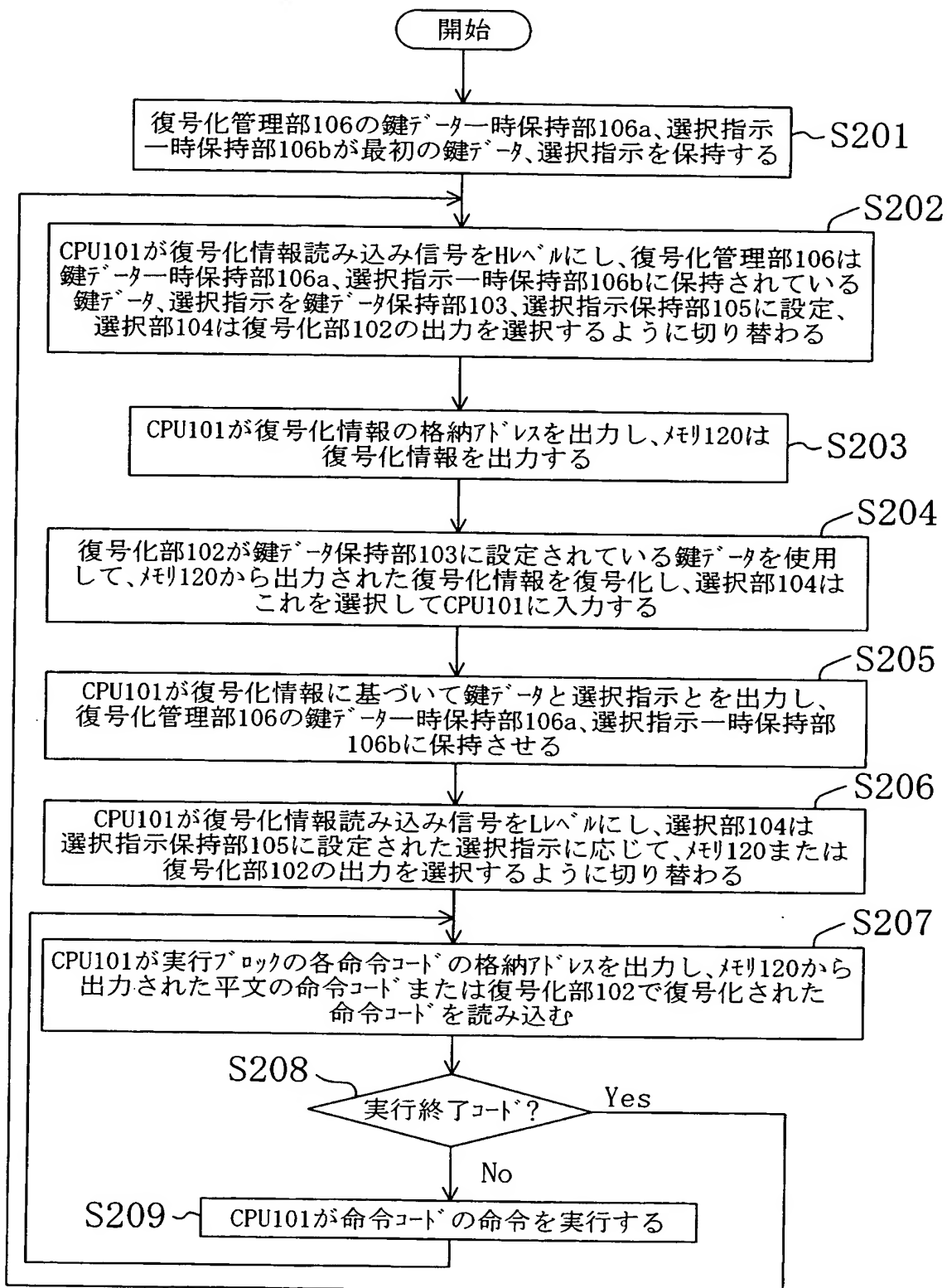
【図3】



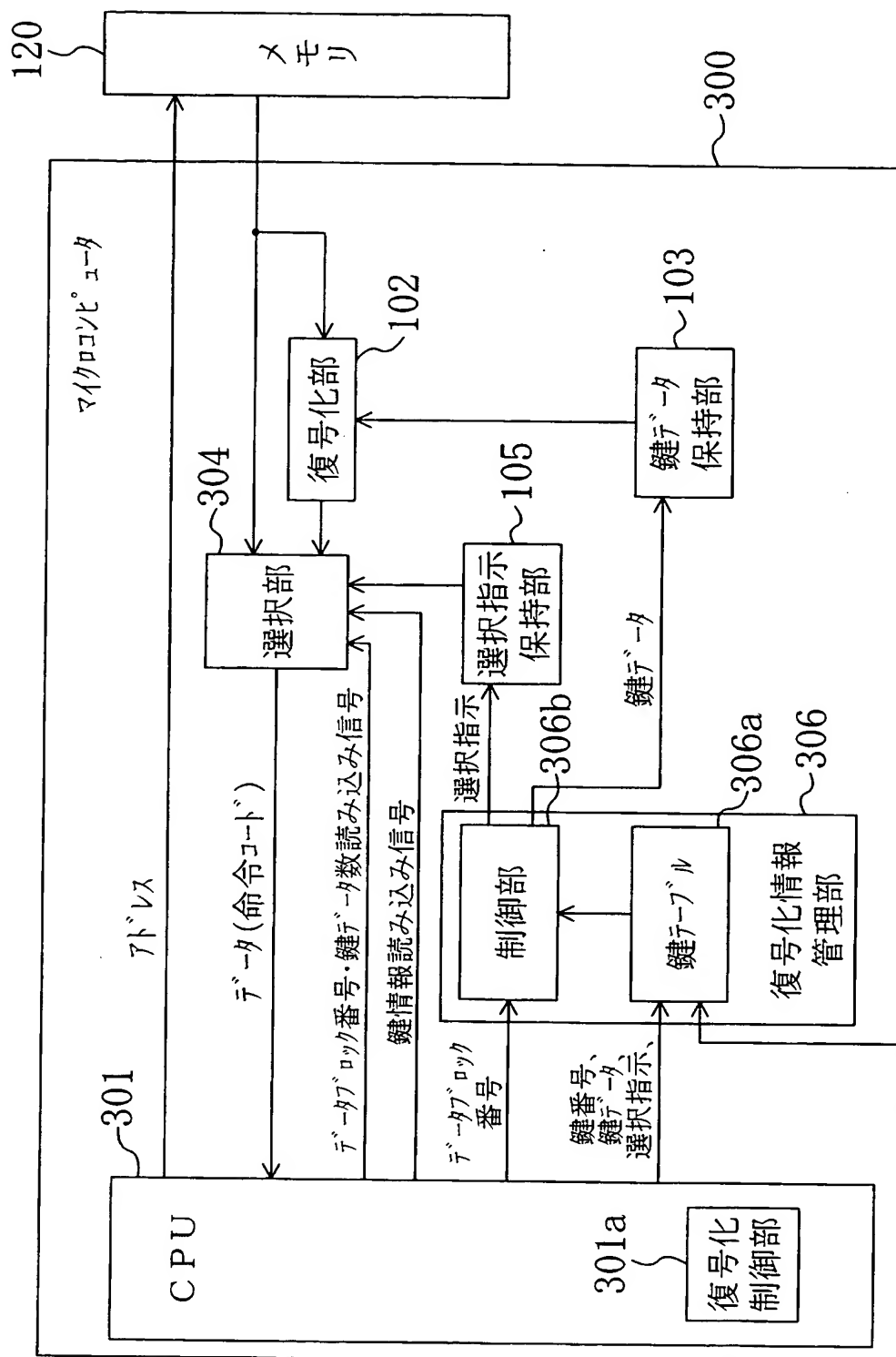
【図 4】



【図5】



【図 6】



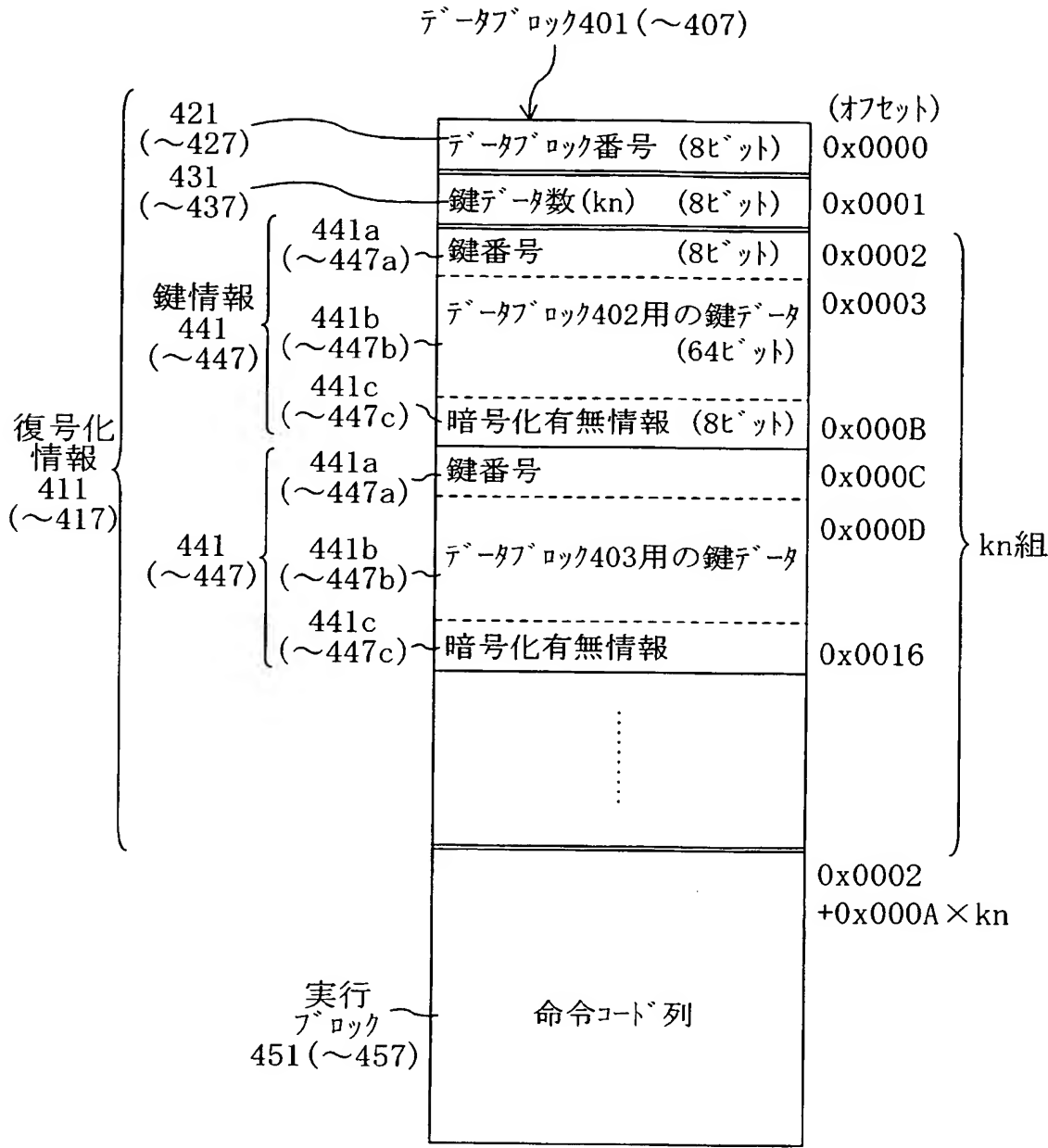
外部からの初期の
鍵番号、鍵データ、選択指示(データブロック401用の鍵番号440a、鍵データ440b、選択指示)

【図 7】

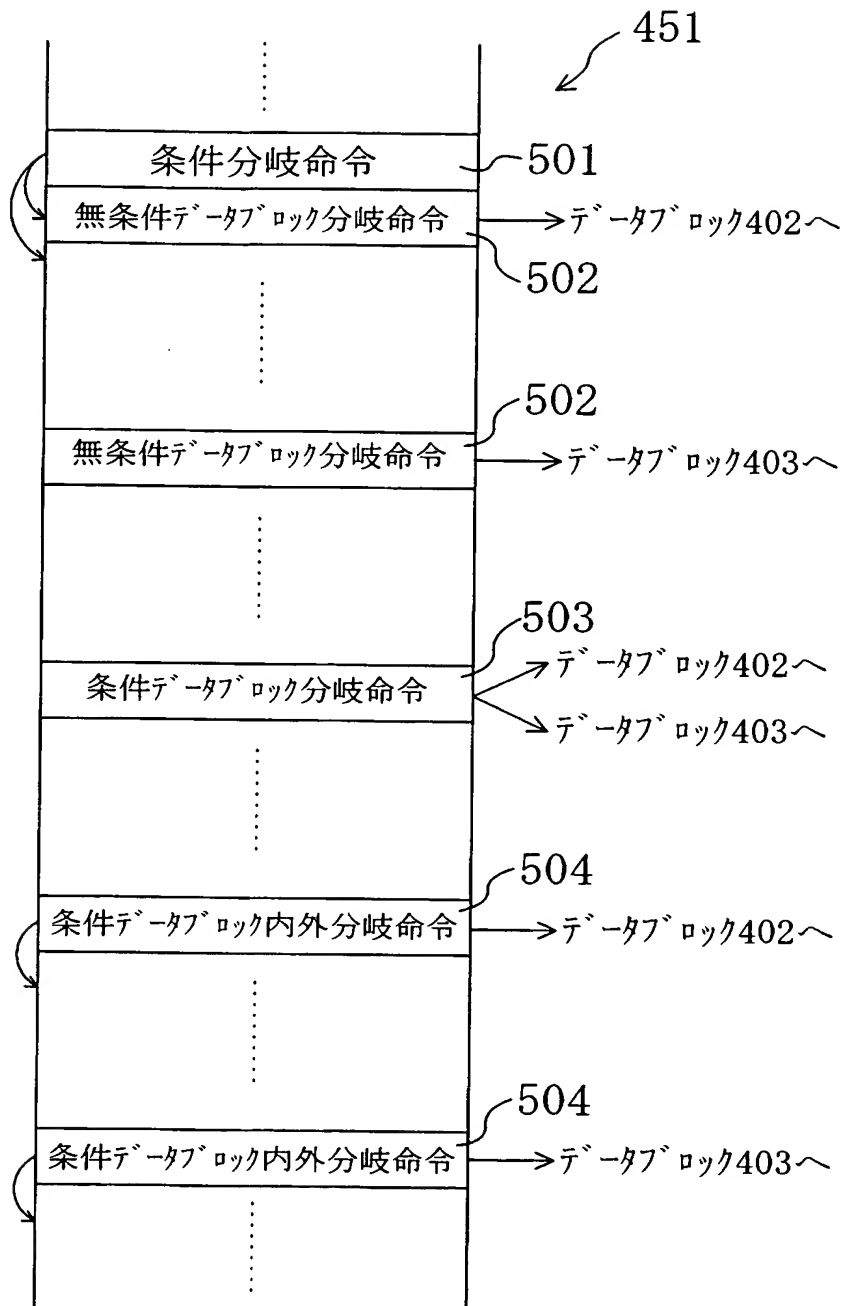
鍵テーブル306aの保持内容

鍵番号	鍵データ	選択指示
0x01	0x1111111111...	1
0x02	0x2222222222...	1
0x03	0x3333333333...	0
⋮	⋮	⋮
0x00	0	0
0x00	0	0

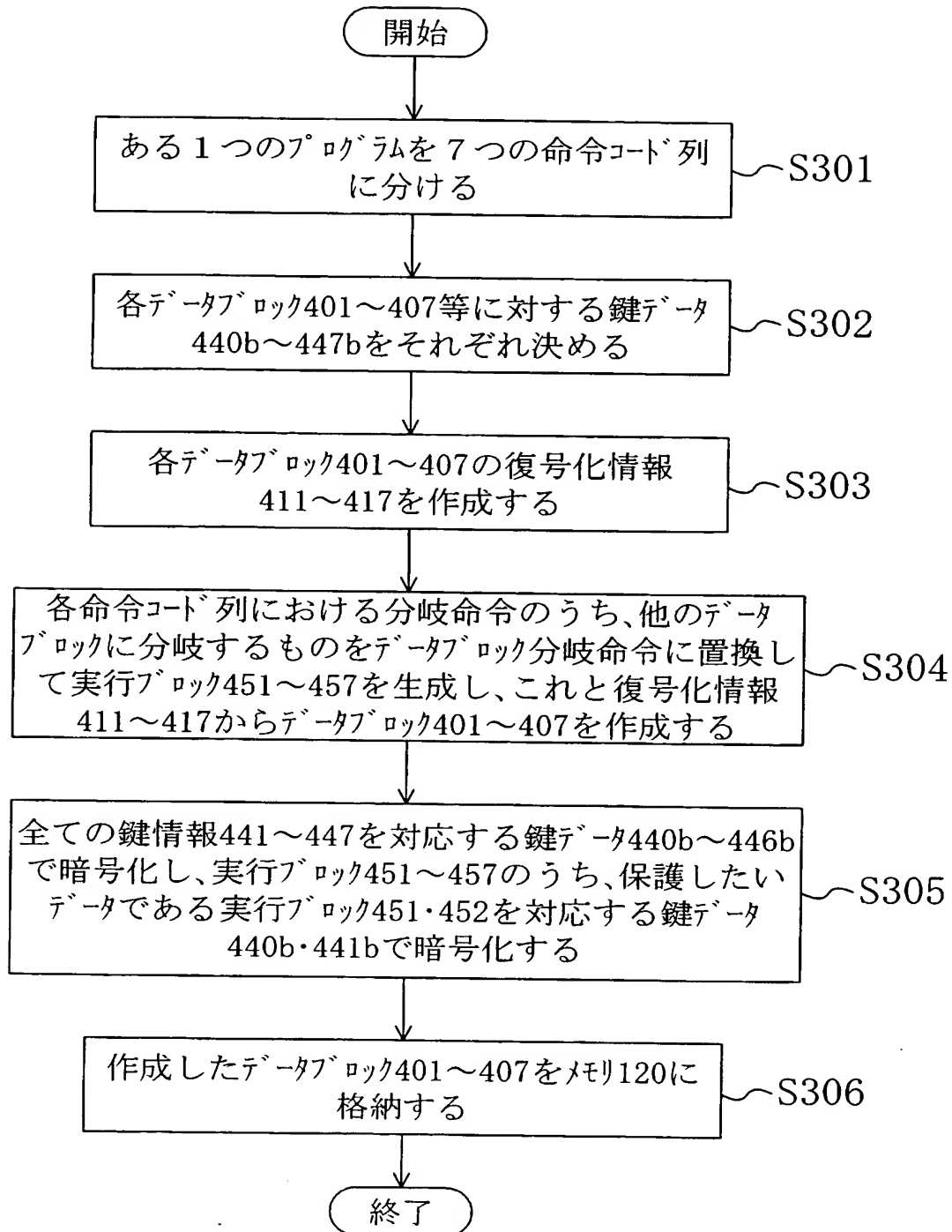
【図 8】



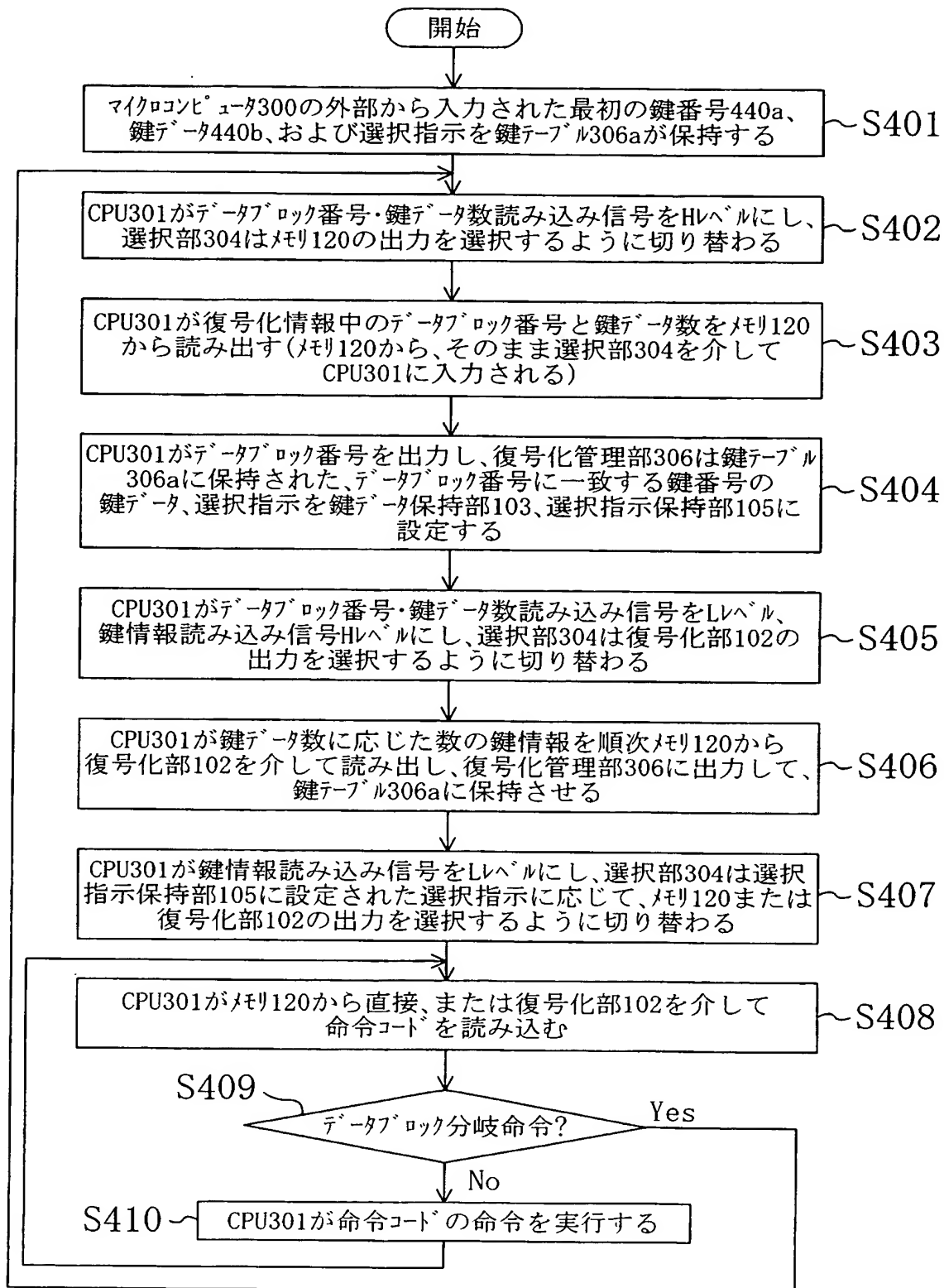
【図 9】



【図 10】

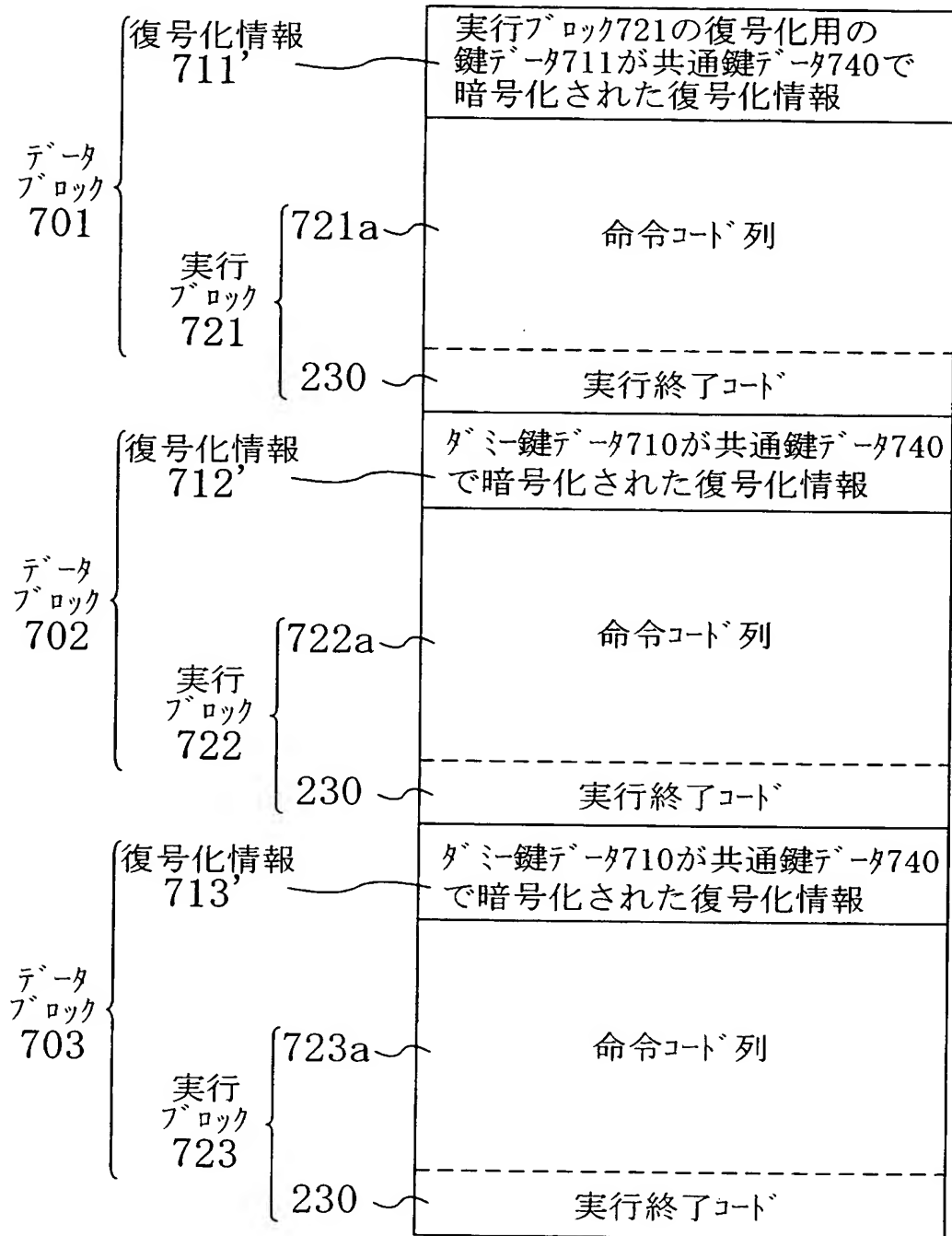


【図 11】

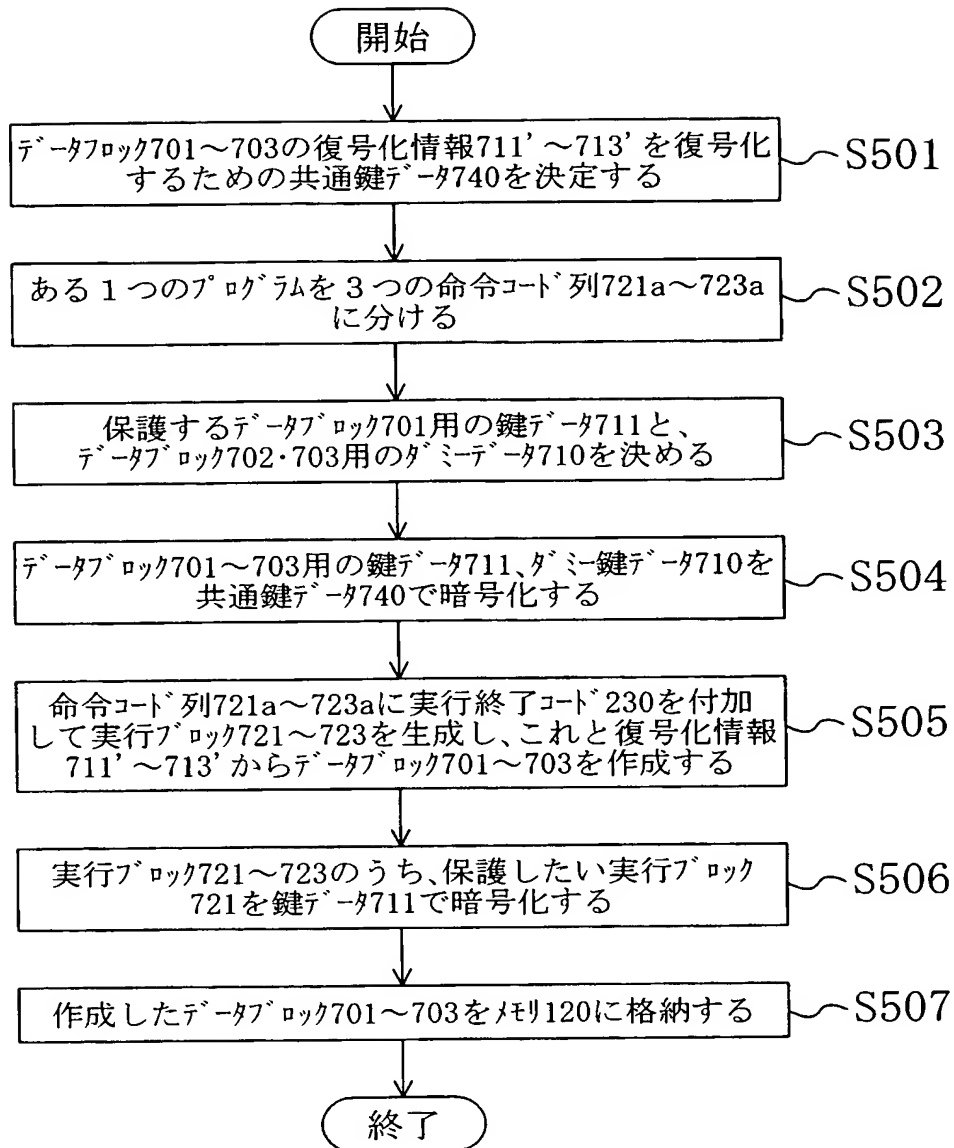


【図 12】

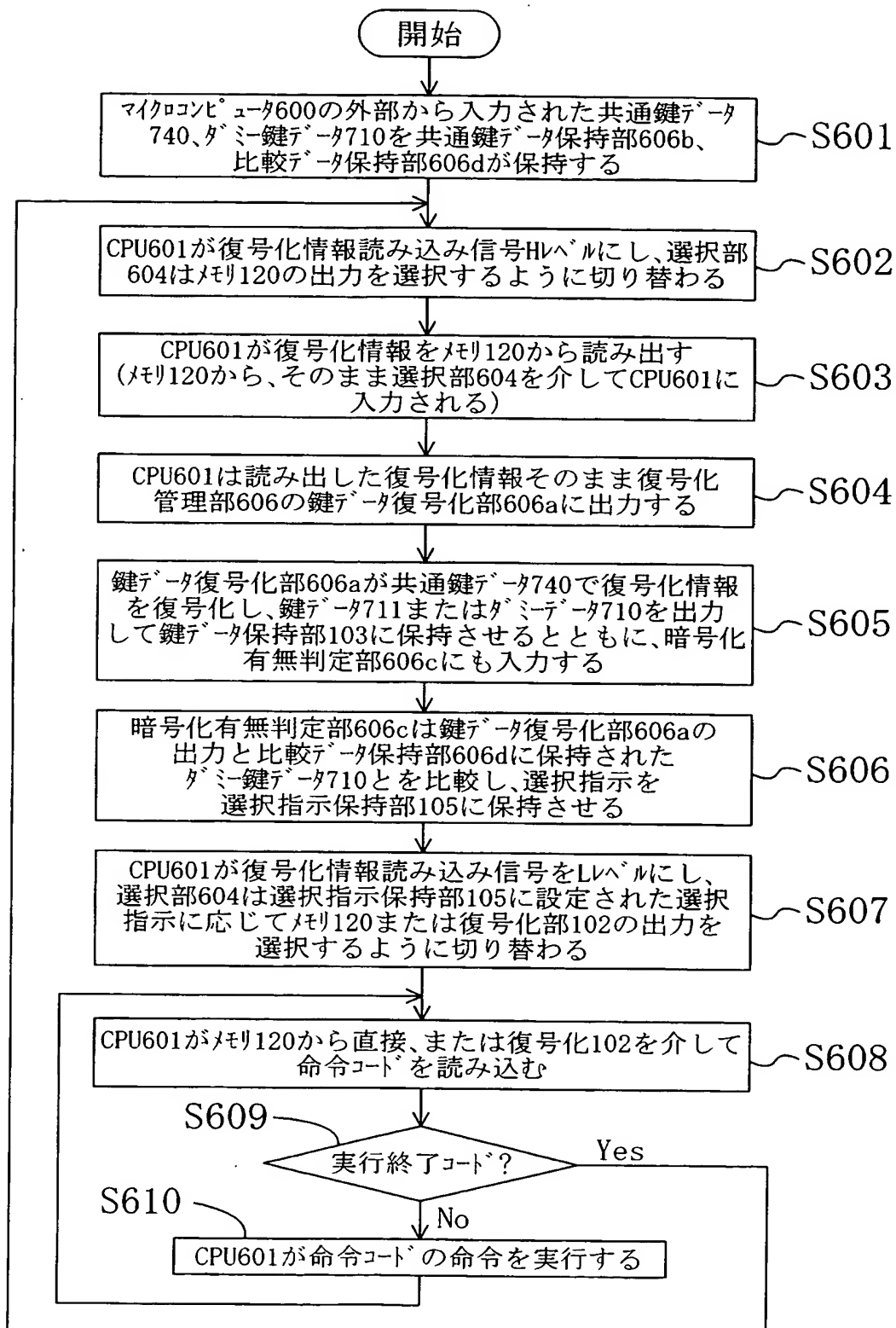
メモリ120に記憶されるデータブロック701～703



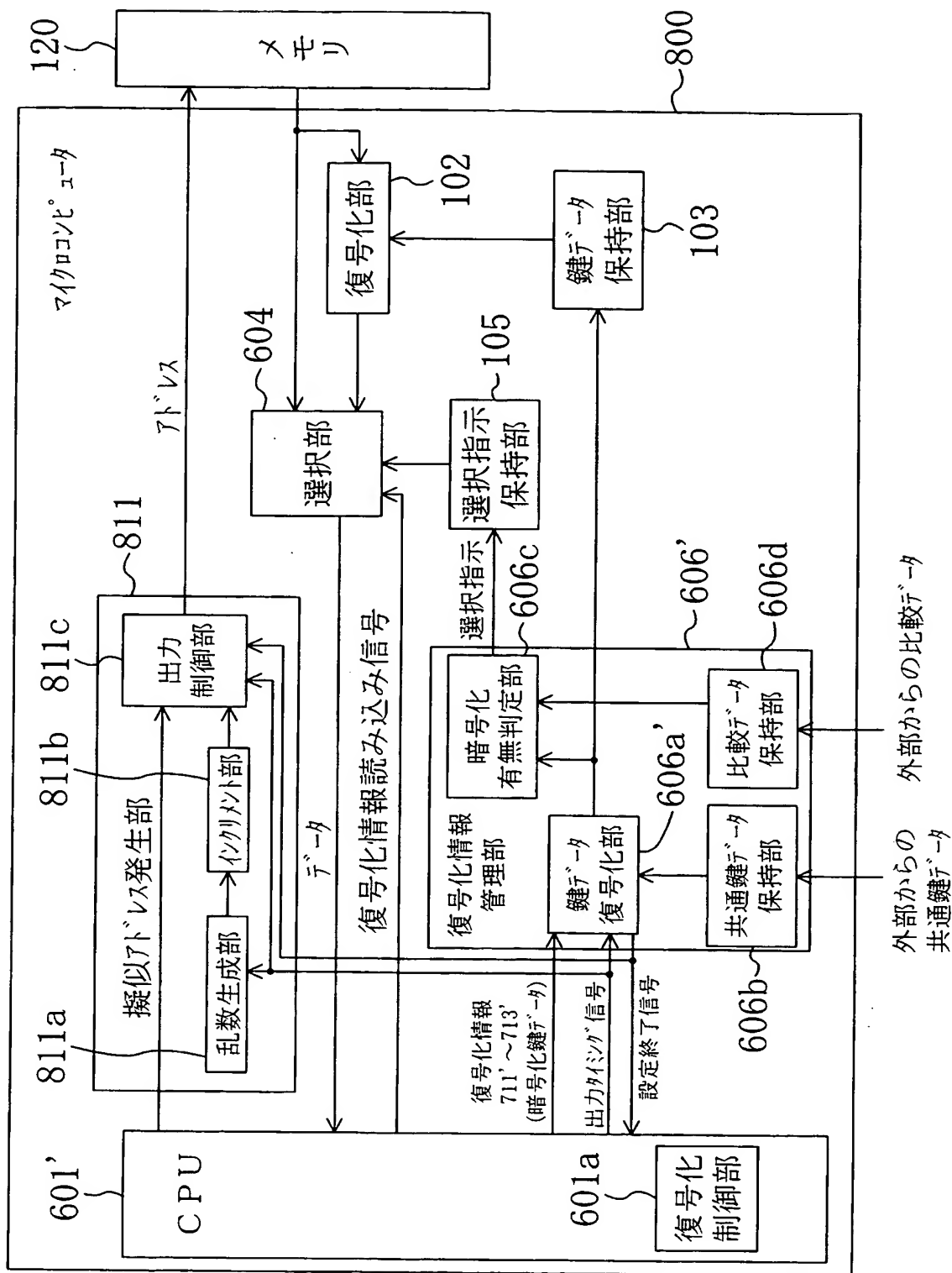
【図 14】



【図 15】



【図 16】



【書類名】 要約書

【要約】

【課題】 復号化鍵の管理を複雑化することなく、記憶データの秘匿性を高める。

【解決手段】 メモリ 1 2 0 に記憶される各データブロックは、元のプログラムが分割されて、それぞれ異なる鍵データで暗号化された実行ブロックと、次に読み込まれるデータブロックを復号化するための暗号化された鍵データを含む復号化情報とを含んでいる。上記データブロックがマイクロコンピュータ 1 0 0 に読み込まれると、復号化部 1 0 2 により復号化された復号化情報中の鍵データは鍵データ一時保持部 1 0 6 a に保持された後、次のデータブロックが読み込まれる際に鍵データ保持部 1 0 3 に保持される。そこで、上記復号化され保持された鍵データによって、次のデータブロックの復号化情報および実行ブロックが復号化される。

【選択図】 図 1

特願 2 0 0 3 - 0 5 5 6 2 6

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社